RSNI3

Rancangan Standar Nasional Indonesia 3

RSNI3 ISO/IEC 29147:2018
(Ditetapkan oleh BSN tahun 2024)

Teknologi informasi – Teknik keamanan – Pengungkapan kerentanan

Information technology – Security techniques – Vulnerability disclosure

(ISO/IEC 29147:2018, IDT)

Pengguna dari RSNI ini diminta untuk menginformasikan adanya hak paten dalam dokumen ini, bila diketahui, serta memberikan informasi pendukung lainnya (pemilik paten, bagian yang terkena paten, alamat pemberi paten dan lain-lain)

ICS 35.030

BADAN STANDARDISASI NASIONAL

BSN
Email: dokinfo@bsn.go.id
www.bsn.go.id

Diterbitkan di Jakarta

Daftar Isi

Prakata

SNI ISO/IEC 29147:2018, Teknologi informasi – Teknik keamanan – Pengungkapan kerentanan, merupakan standar yang disusun dengan jalur adopsi tingkat keselarasan identik dari ISO/IEC 29147:2018 *Information technology – Security techniques – Vulnerability disclosure*, dengan metode adopsi terjemahan dua bahasa dan ditetapkan oleh BSN pada tahun 2024.

Standar ini disusun oleh Komite Teknis 35-04, Keamanan Informasi, Keamanan Siber dan Perlindungan Privasi. Standar ini telah dibahas melalui rapat teknis dan disepakati dalam rapat konsensus pada tanggal 21 Juni 2024 di Depok, yang dihadiri oleh para pemangku kepentingan *(stakeholder)* terkait yaitu perwakilan dari pemerintah, pelaku usaha, konsumen, dan pakar. Standar ini telah melalui tahap jajak pendapat pada tanggal 18 Juli 2024 sampai dengan 1 Agustus 2024 dengan hasil akhir disetujui menjadi SNI.

Kosakata yang digunakan dalam Standar ini mengikuti bentuk baku yang dicantumkan dalam Kamus Besar Bahasa Indonesia (KBBI), tetapi ada beberapa kosakata yang belum ada di dalam KBBI.

Kata/istilah "*patch*", "*cloud*", *"SQL injection", "cross-site scripting", "bug",* dan *"feeds"* tidak diterjemahkan dalam Standar ini karena Komite Teknis 35-04 belum menemukan padanan kata/istilah yang sesuai dengan konteks yang sesuai dalam Bahasa Indonesia.

Apabila pengguna menemukan keraguan dalam standar ini maka disarankan untuk melihat standar aslinya yaitu ISO/IEC 29147:2018, dan/atau dokumen terkait lain yang menyertainya.

Perlu diperhatikan bahwa kemungkinan beberapa unsur dari standar ini dapat berupa hak kekayaan intelektual (HAKI). Namun selama proses perumusan SNI, Badan Standardisasi Nasional telah memperhatikan penyelesaian terhadap kemungkinan adanya HAKI terkait substansi SNI. Apabila setelah penetapan SNI masih terdapat permasalahan terkait HAKI, Badan Standardisasi Nasional tidak bertanggung jawab mengenai bukti, validitas, dan ruang lingkup dari HAKI tersebut.

Pendahuluan

Dalam konteks teknologi informasi dan keamanan siber, kerentanan adalah perilaku atau set dari kondisi yang ada dalam sebuah sistem, produk, komponen, atau layanan yang melanggar kebijakan keamanan yang implisit atau eksplisit. Kerentanan dapat dianggap sebagai kelemahan atau paparan yang memungkinkan adanya dampak atau konsekuensi keamanan. Penyerang mengeksploitasi kerentanan untuk pembobolan konfidensialitas, integritas, availabilitas, operasi, atau properti keamanan lainnya.

Kerentanan sering dihasilkan dari kegagalan program atau sistem dalam menangani input yang taktepercaya atau takterduga secara aman. Penyebab yang menyebabkan kerentanan termasuk galat dalam pengodean atau konfigurasi, kelalaian dalam pilihan desain, dan spesifikasi protokol dan format yang tidak aman.

Meskipun terdapat upaya yang signifikan untuk meningkatkan keamanan perangkat lunak, perangkat lunak dan sistem modern sangatlah kompleks sehingga pada praktiknya tidak mungkin untuk memproduksinya tanpa kerentanan. Faktor risiko kerentanan meliputi:

— mengoperasikan dan mengandalkan sistem yang memiliki kerentanan yang diketahui;

— tidak memiliki informasi yang memadai tentang kerentanan;

— tidak mengetahui bahwa ada kerentanan.

Dokumen ini menjelaskan pengungkapan kerentanan: teknik dan kebijakan bagi vendor untuk menerima laporan kerentanan dan memublikasikan informasi remediasi. Pengungkapan kerentanan memampukan remediasi kerentanan dan pengambilan keputusan risiko yang lebih tepat. Pengungkapan kerentanan adalah elemen kritikal pada dukungan, pemeliharaan, dan pengoperasian produk atau layanan apa pun yang terkena ancaman aktif. Hal ini mencakup hampir semua produk atau layanan yang menggunakan jaringan terbuka seperti Internet. Kapabilitas pengungkapan kerentanan merupakan bagian esensial dari pengembangan, akuisisi, pengoperasian, dan dukungan semua produk dan layanan. Beroperasi tanpa kapabilitas pengungkapan kerentanan menempatkan pengguna pada peningkatan risiko.

Istilah “pengungkapan kerentanan” digunakan untuk menjelaskan keseluruhan aktivitas yang berasosiasi dengan penerimaan laporan kerentanan dan penyediaan informasi remediasi. Aktivitas tambahan seperti investigasi dan pemrioritasan laporan, pengembangan, pengetesan, dan penerapan remediasi, serta peningkatan pengembangan yang aman disebut sebagai “penanganan kerentanan” dan dideskripsikan dalam ISO/IEC 30111. Istilah “pengungkapan” juga digunakan secara lebih sempit untuk mengartikan tindakan menginformasikan suatu pihak tentang kerentanan untuk pertama kalinya (lihat 3.2).

Gol utama pengungkapan kerentanan meliputi:

— mengurangi risiko dengan meremediasi kerentanan dan menginformasikan pengguna;

— meminimalisasi kerugian dan biaya yang berasosiasi dengan pengungkapan;

— menyediakan informasi yang cukup kepada pengguna untuk mengevaluasi risiko akibat kerentanan;

— mengeset ekspektasi untuk memfasilitasi interaksi dan koordinasi kooperatif di antara para pemangku kepentingan.

Proses yang dideskripsikan dalam dokumen ini bertujuan untuk meminimalkan risiko, biaya, dan kerugian bagi semua pemangku kepentingan. Karena volume kerentanan yang dilaporkan, kurangnya informasi yang akurat dan lengkap, serta faktor lain yang terlibat, maka tidak mungkin untuk membuat proses tunggal yang tetap yang berlaku untuk setiap kejadian pengungkapan.

Elemen normatif dalam dokumen ini menyediakan persyaratan minimum untuk menciptakan kapabilitas pengungkapan kerentanan yang fungsional. Vendor sebaiknya menyesuaikan panduan informatif tambahan dalam dokumen ini agar sesuai dengan kebutuhan khusus mereka dan kebutuhan pengguna serta pemangku kepentingan lainnya.

Teknologi informasi — Teknik keamanan — Pengungkapan kerentanan

1 Ruang lingkup

Dokumen ini menyediakan persyaratan dan rekomendasi kepada vendor mengenai pengungkapan kerentanan pada produk dan layanan. Pengungkapan kerentanan memungkinkan pengguna untuk melakukan manajemen kerentanan teknis seperti yang ditentukan dalam ISO/IEC 27002:2013, 12.6.1[1]. Pengungkapan kerentanan membantu pengguna memproteksi sistem dan data mereka, memprioritaskan investasi defensif, dan menilai risiko dengan lebih baik. Tujuan pengungkapan kerentanan adalah untuk mengurangi risiko yang berkaitan dengan eksploitasi kerentanan. Pengungkapan kerentanan yang terkoordinasi sangat penting terutama ketika multipel vendor terdampaknya. Dokumen ini menyediakan:

— pedoman dalam penerimaan laporan tentang potensi kerentanan;

— pedoman dalam pengungkapan informasi remediasi kerentanan;

— istilah dan definisi yang spesifik untuk pengungkapan kerentanan;

— gambaran umum tentang konsep pengungkapan kerentanan;

— pertimbangan teknik dan kebijakan untuk pengungkapan kerentanan;

— contoh teknik, kebijakan (Lampiran A), dan komunikasi (Lampiran B).

Aktivitas terkait lainnya yang berlangsung antara penerimaan dan pengungkapan laporan kerentanan dideskripsikan dalam ISO/IEC 30111.

Dokumen ini berlaku bagi vendor yang memilih mempraktikkan pengungkapan kerentanan untuk mengurangi risiko terhadap pengguna produk dan layanan vendor.

2 Acuan normatif

Dokumen-dokumen berikut dirujuk dalam teks sedemikian rupa sehingga sebagian atau semua isinya merupakan persyaratan dokumen ini. Untuk acuan bertanggal, hanya edisi yang dikutip yang berlaku. Untuk acuan yang tidak bertanggal, berlaku edisi terakhir dari dokumen acuan tersebut (termasuk setiap amendemennya).

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*

3 Istilah dan definisi

Untuk tujuan dokumen ini, istilah dan definisi yang tersedia dalam ISO/IEC 27000 dan istilah – istilah berikut ini berlaku.

ISO dan IEC memelihara basis data terminologi untuk digunakan dalam standardisasi di

alamat berikut:

— ISO *Online browsing platform*: tersedia di https:// www.iso.org/obp

— IEC Electropedia: tersedia di https://www.electropedia.org/

3.1
kerentanan
perilaku fungsional produk atau layanan yang melanggar kebijakan keamanan implisit atau eksplisit

Catatan 1 untuk entri: ISO/IEC 27002:2013, 12.6.1[1] menggunakan istilah “kerentanan teknis” untuk membedakan antara konsep kerentanan berbasis risiko yang lebih umum dan istilah yang digunakan dalam dokumen ini.

3.2
pengungkapan
tindakan penyediaan informasi kerentanan (3.1) di awal kepada pihak yang tidak diyakini menyadari sebelumnya.

3.3
koordinasi
serangkaian aktivitas termasuk mengidentifikasi dan melibatkan pemangku kepentingan, memediasi, mengkomunikasikan, dan perencanaan lainnya dalam mendukung pengungkapan (3.2) kerentanan (3.1)

Catatan 1 untuk entri: Istilah “pengungkapan kerentanan terkoordinasi” digunakan untuk menunjukkan proses pengungkapan yang mencakup koordinasi.

3.4
vendor
individu atau organisasi yang bertanggung jawab untuk meremediasi kerentanan

Catatan 1 untuk entri: Vendor dapat berupa developer, pemelihara, produsen, pabrikan, pemasok, penginstal, atau penyedia produk atau layanan.

3.5
pelapor
individu atau organisasi yang memberikan notifikasi kepada vendor (3.4) atau koordinator (3.6) tentang potensi kerentanan (3.1)

Catatan 1 untuk entri: Tidak ada persyaratan khusus untuk bertindak sebagai pelapor. Pelapor dapat berupa individu, organisasi, amatir atau penggemar, professional, pengguna akhir, organisasi riset keamanan, vendor, pemerintah, atau koordinator.

Catatan 2 untuk entri: Istilah “pelapor” tidak berarti penemuan atau pelaporan yang unik atau orisinal.

Catatan 3 untuk entri: Pelapor dapat disebut sebagai peneliti, baik pelapor tersebut secara eksplisit melakukan riset keamanan atau kerentanan maupun tidak. Secara historis, peran ini juga disebut sebagai “penemu”.

3.6
koordinator
individu atau organisasi yang melakukan koordinasi (3.3)

3.7
remediasi
perubahan yang dilakukan pada produk atau layanan untuk menghilangkan atau memitigasi kerentanan (3.1)

Catatan 1 untuk entri: Remediasi biasanya berupa penggantian fail biner, perubahan konfigurasi, atau *patch* kode sumber dan kompilasi ulang. Istilah berbeda yang digunakan untuk “remediasi” termasuk *patch*, perbaikan, pembaruan, perbaikan terbaru, dan peningkatan. Mitigasi juga disebut solusi sementara atau tindakan penanggulangan.

3.8
advisori
dokumen atau pesan yang menyediakan informasi kerentanan (3.1) yang dimaksudkan untuk mengurangi risiko

Catatan 1 untuk entri: Advisori dimaksudkan untuk menginformasikan pengguna atau pemangku kepentingan lainnya tentang kerentanan, termasuk, jika mungkin, bagaimana mengidentifikasi dan meremediasi sistem yang rentan

4 Istilah singkatan

COTS	produk perangkat lunak yang umum tersedia secara luas di pasar (*common off-the-shelf*)
CRM	manajemen hubungan pelanggan (*customer relationship management*)
CSIRT	tim tanggap insiden keamanan komputer (*computer security incident response team*)
CVE	kerentanan dan eksposur umum (*common vulnerabilities and exposures*[9])
CVRF	format pelaporan kerentanan umum (*common vulnerability reporting format*[12][13])
CVSS	sistem penilaian kerentanan umum (*common vulnerability scoring system*[10])
CWE	enumerasi kelemahan umum (*common weakness enumeration*[11])
HTTP(S)	protokol transfer hiperteks (aman) (*hypertext transfer protocol (secure)*)
ICT	teknologi informasi dan komunikasi (*information and communication technology*)
OpenPGP	keamanan cukup baik terbuka (*open pretty good privacy*)
OWASP	proyek keamanan aplikasi web terbuka (*open web application security project*)
PoC	bukti dari konsep (*proof of concept*)
PSIRT	tim tanggap insiden keamanan produk (*product security incident response team*)
S/MIME	ekstensi surat internet serbaguna yang aman (*secure multipurpose internet mail extensions*)
SQL	bahasa kueri terstruktur (*structured query language*)
TLS	keamanan lapisan transportasi (*transport layer security*)

5 Konsep

5.1 Umum

Tujuan pasal ini adalah untuk menyediakan informasi latar belakang dan konteks untuk membantu memahami pengungkapan kerentanan.
Pengungkapan kerentanan melibatkan pemangku kepentingan yang berbeda dengan perspektif, insentif, kapabilitas, dan informasi tersedia yang berbeda. Selain itu, komunikasi dan sinkronisasi proses di antara multipel pemangku kepentingan dapat menjadi rumit dengan cepat. Pada praktiknya, pengungkapan dapat menyimpang dari aktivitas yang dideskripsikan dalam dokumen ini karena berbagai keadaan yang tidak terduga.

5.2 Struktur dokumen ini

Dokumen ini dimaksudkan untuk dibaca secara keseluruhan sebagai input pada pengembangan atau peningkatan kebijakan dan proses pengungkapan kerentanan. Pasal lainnya dalam dokumen ini disusun sebagai berikut:

— Pasal 5: Konsep;

— Pasal 6: Penerimaan laporan kerentanan;

— Pasal 7: Pemublikasian advisori kerentanan;

— Pasal 8: Koordinasi;

— Pasal 9: Kebijakan pengungkapan kerentanan.

Struktur dokumen ini tidak dimaksudkan untuk diikuti dalam urutan yang ketat seperti yang tampak di atas. Sebagai contoh, vendor sebaiknya secara ideal mengembangkan kebijakan (Pasal 9) sebelum mulai menerima laporan (Pasal 6).

Lampiran D berisi ringkasan semua elemen normatif dalam dokumen ini.

5.3 Hubungan dengan Standar Internasional lainnya

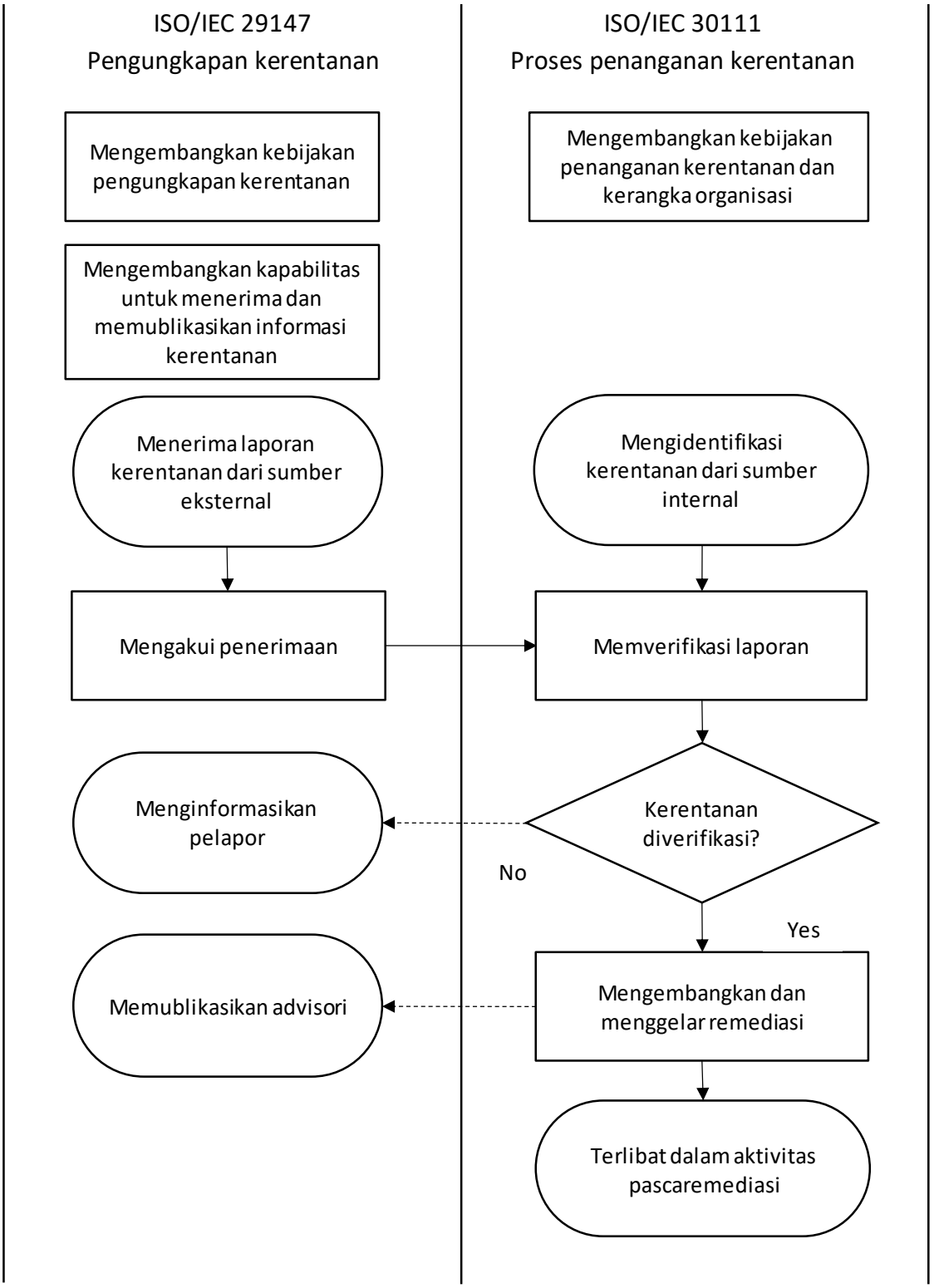
5.3.1 ISO/IEC 30111

ISO/IEC 30111 harus digunakan secara bersamaan dengan dokumen ini. Hubungan antara kedua Standar Internasional tersebut diilustrasikan pada Gambar 1.

Dokumen ini menyediakan pedoman bagi vendor untuk disertakan dalam proses bisnis normal mereka ketika menerima laporan tentang potensi kerentanan dari individu atau organisasi eksternal dan ketika mendistribusikan informasi remediasi kerentanan kepada pengguna yang terdampak.

ISO/IEC 30111 memberikan pedoman tentang cara menginvenstigasi, memproses, dan menyelesaikan laporan potensi kerentanan.

Sementara dokumen ini berurusan dengan antarmuka antara vendor dan pelapor, ISO/IEC 30111 berurusan dengan proses internal vendor termasuk triase, investigasi, dan remediasi kerentanan, baik sumber laporan berasal dari luar vendor maupun dari dalam tim keamanan, pengembangan, atau pengujian vendor.



Gambar 1 — Hubungan antara ISO/IEC 29147 dan ISO/IEC 30111

5.3.2 ISO/IEC 27002

Pengungkapan kerentanan memberdayakan manajemen kerentanan teknis (ISO/IEC 27002:2013, 12.6.1[1]).

5.3.3 Seri ISO/IEC 27034

Keamanan aplikasi berupaya mengurangi terciptanya kerentanan aplikasi (lihat ISO/IEC 27034-1:2011, 6.5.2[4]). Pengungkapan kerentanan dapat menunjukkan perlunya perubahan pada praktik keamanan aplikasi. Pengungkapan kerentanan tidak dapat menunjukkan bahwa keamanan aplikasi sepenuhnya efektif.

Pengungkapan kerentanan terjadi pada fase utilisasi dan pemeliharaan model referensi siklus hidup keamanan aplikasi yang dideskripsikan dalam ISO/IEC TS 27034-5-1:2018, 6.3.13 and 6.3.14[5].

5.3.4 ISO/IEC 27036-3

Pengungkapan kerentanan mendukung multipel aspek keamanan rantai pasokan ICT yang dideskripsikan dalam ISO/IEC 27036-3:2013, 5.4 a), 5.8 i), 6.1.1 a) 2) and 6.3.4 [7].

5.3.5 ISO/IEC 27017

Pengungkapan kerentanan diperlukan untuk memberdayakan manajemen kerentanan teknis sebagaimana ditentukan untuk layanan *cloud* dalam ISO/IEC 27017:2015, 12.6.1[3].

5.3.6 Seri ISO/IEC 27035

Beberapa rencana manajemen insiden, khususnya pada vendor, mencakup pengungkapan kerentanan (lihat ISO/IEC 27035-1:2016, Pendahuluan[6]). Rencana seperti ini biasanya memperlakukan pengungkapan kerentanan sebagai tipe insiden. Manajemen insiden juga dapat mencakup manajemen kerentanan (lihat juga ISO/IEC 27002:2013, 12.6.1[1]), yang hanya mungkin terjadi jika kerentanan terungkap.

5.3.7 Evaluasi, pengujian dan spesifikasi keamanan

Dokumen ini menyediakan panduan untuk laporan kerentanan yang diterima secara eksternal, dan bukan melalui upaya pemastian dan evaluasi internal yang terorganisasi. Oleh karena itu, standar pengujian, pemastian, dan evaluasi ISO/IEC 15408[15] dan ISO/IEC 18405[16] yang lebih formal tidak berlaku secara umum.

5.4 Sistem, komponen, dan layanan

5.4.1 Sistem

Sistem adalah serangkaian komponen dan layanan yang terkoneksi. Pada pengungkapan kerentanan, penyebab suatu kerentanan dapat tidak jelas, atau karena interaksi antar bagian pada sistem, atau antar sistem. Oleh karena itu, terkadang perlu untuk membicarakan tentang sistem yang terdampak oleh kerentanan.

5.4.2 Komponen

Komponen adalah unit perangkat lunak atau perangkat keras yang dapat berupa keseluruhan sistem tersendiri dan digunakan sebagai bagian dari sistem yang lebih besar. Komponen dapat berupa sistem operasi keseluruhan, cip, aplikasi, paket, pustaka, atau bahkan dokumen tunggal atau segmen kode sumber.

Untuk tujuan dokumen ini, pembedaan antara komponen perangkat keras dan perangkat lunak jarang relevan. Terdapat sangat sedikit kasus kerentanan pada komponen perangkat keras

murni. Dalam kebanyakan kasus, apa yang disebut kerentanan “perangkat keras” sebenarnya terjadi pada perangkat lunak atau perangkat tegar (*firmware*) level rendah.

5.4.3 Produk

Produk biasanya berupa satu atau beberapa komponen atau sistem. Produk disediakan oleh vendor kepada pengguna untuk dijual atau gratis, biasanya berdasarkan ketentuan lisensi. Terdapat banyak tipe produk berbeda termasuk tetapi tidak terbatas pada, perangkat lunak khusus yang dibuat berdasarkan kontrak untuk penggunaan berlisensi pengguna tertentu, pustaka yang dimaksudkan untuk disertakan dalam produk lainnya, produk COTS (*commercial off-the-shelf*) untuk pasar massal, proyek yang dikembangkan komunitas, dan penawaran produk hiburan atau hobi.

5.4.4 Layanan

Layanan adalah kumpulan fitur yang disediakan untuk pengguna. Pengguna dapat berinteraksi dengan layanan yang tidak mereka miliki, operasikan, atau pelihara.
Untuk pengungkapan kerentanan, kerentanan pada layanan yang dipelihara oleh vendor biasanya dapat diremediasi oleh vendor yang mengambil tindakan. Pengguna dapat juga diharuskan mengambil tindakan untuk meremediasi kerentanan. Misalnya, vendor mengimplementasikan perubahan pada infrastuktur mereka untuk meremediasi kerentanan, dan pengguna harus mengubah kata sandi mereka setelah vendor mengimplementasikan perubahan tersebut.

5.4.5 Kerentanan

Kerentanan secara umum merupakan perilaku atau serangkaian kondisi yang memungkinkan pelanggaran terhadap kebijakan keamanan eksplisit atau implisit. Biasanya, pelanggaran terhadap kebijakan keamanan pengguna mengakibatkan dampak negatif atau kerugian kepada pengguna. Satu cara umum untuk mengategorikan kerugian adalah mempertimbangkan dampaknya terhadap konfidensialitas, integritas, dan availabilitas aset. Misalnya, kerentanan yang memungkinkan penyerang menginstal perangkat lunak berbahaya pada sistem pengguna akan berdampak pada konfidensialitas dan integritas karena penyerang dapat menggunakan perangkat lunak berbahaya untuk membaca atau mengubah informasi sensitif. Kerentanan pada produk jaringan yang menyebabkan produk mengalami kesalahan sistem akan berdampak pada availabilitas. Dampak sebenarnya kerentanan bergantung pada bagaimana produk yang rentan tersebut digunakan dan faktor kontekstual lainnya.

Kerentanan sering disebabkan oleh cacat implementasi pada perangkat lunak. Kerentanan dapat diasosiasikan dengan kebijakan keamanan jika ada. Satu tipe umum dari kerentanan termasuk *buffer overflow* dan kesalahan manajemen memori tingkat rendah yang memungkinkan input dibuat secara khusus untuk mengontrol eksekusi program perangkat lunak yang rentan. Kerentanan *SQL Injection* dan *cross-site scripting* adalah tipe umum kerentanan yang ditemukan pada aplikasi web. Banyak rangkaian kondisi lain yang dapat menyebabkan atau berkontribusi terhadap kerentanan, termasuk keputusan desain, pengaturan konfigurasi bawaan, autentikasi atau akses kontrol yang lemah, kurangnya kesadaran atau edukasi, atau bahkan interaksi yang tidak terduga antar sistem atau perubahan dalam lingkungan pengoperasian.

Informasi lebih lanjut tentang tipe kerentanan dapat ditemukan dalam CWE dan OWASP. Kedua sumber ini membantu developer dan teknisi untuk mengenali dan menghindari terciptanya kerentanan keamanan.

Banyak pemangku kepentingan (terutama vendor dan pengguna) berupaya untuk

mengidentifikasi dan menyelesaikan kerentanan, dengan menghilangkan kerentanan tersebut seluruhnya (biasanya dengan *patching* atau pembaharuan perangkat lunak untuk menghilangkan cacat) atau dengan memitigasi atau mengatasi kerentanan untuk mengurangi kemungkinan atau dampak serangan yang berhasil. Pengungkapan kerentanan menyediakan vendor dan pengguna informasi untuk menyelesaikan dan memitigasi kerentanan serta membuat keputusan risiko yang lebih baik.

Penyerang juga berupaya untuk mengidentifikasi kerentanan, tetapi biasanya tidak mencoba untuk mengungkap atau menyelesaikan kerentanan. Penyerang berupaya untuk mengeksploitasi kerentanan untuk mendapatkan keuntungan, hampir selalu menyebabkan kerugian terhadap pengguna.

5.4.6 Interdependensi produk

Banyak produk merupakan sistem kompleks yang mencakup atau bergantung pada produk atau komponen lain dalam beberapa cara. Ada kemungkinan bahwa pengguna atau vendor pada awalnya tidak yakin produk yang terdampak kerentanan. Interdependensi ini penting karena produk yang menggunakan atau berinteraksi dengan produk yang rentan dapat juga menjadi rentan.

Dependensi produk dapat mencakup:

— penggunaan ulang kode sumber dari produk lain, pustaka perangkat lunak, atau tipe antarmuka lainnya;

— rantai pasokan perangkat keras atau perangkat lunak;

— penjenamaan ulang (*rebranding*) oleh vendor yang berbeda dari teknologi inti yang sama;

— penggunaan protokol atau format yang sama.

Bergantung pada model penjualan, distribusi, dan pendukung, vendor dapat memiliki daftar pengguna yang akurat atau tidak. Hal ini mungkin relevan ketika mempertimbangkan untuk memberitahu pengguna yang terdampak kerentanan.

5.5 Peran pemangku kepentingan

5.5.1 Umum

Subpasal ini menjelaskan peran signifikan pemangku kepentingan dalam pengungkapan kerentanan. Pemangku kepentingan adalah individu, grup, atau organisasi yang bertindak dalam satu atau beberapa peran.

5.5.2 Pengguna

Pengguna dapat secara langsung mengoperasikan produk perangkat lunak atau perangkat keras atau memanfaatkan suatu layanan. Pengguna dapat disebut sebagai konsumen, pelanggan, atau pengguna akhir. Karena interdependensi produk perangkat lunak modern, pengguna mungkin tidak mengetahui secara pasti produk atau layanan yang sebenarnya mereka gunakan.

Pengguna membutuhkan informasi tentang kerentanan, khususnya remediasi, untuk membuat keputusan risiko yang efektif serta menggunakan produk dan layanan perangkat lunak secara lebih aman. Pemublikasian informasi kerentanan didiskusikan dalam Pasal 7.

5.5.3 Vendor

Terdapat beberapa istilah berbeda yang digunakan untuk menggambarkan individu atau organisasi yang membuat atau menyediakan produk perangkat lunak, termasuk pabrikan, developer, pemelihara, atau distributor. Demikian pula, individu atau organisasi yang mengirimkan produk perangkat lunak di dalam rantai pasokan dapat disebut sebagai pemasok. Untuk tujuan dokumen ini, istilah “vendor” digunakan untuk merujuk semua individu dan organisasi tersebut. Vendor dapat berupa individu, tim kecil, perusahaan komersial besar, atau sebuah proyek sumber terbuka.

Vendor bertanggung jawab atas keamanan produk dan layanannya. Vendor melakukan pengungkapan kerentanan untuk menerima laporan tentang kerentanan, mengembangkan remediasi, dan memublikasikan advisori.

Terdapat banyak tipe vendor dengan berbagai model dalam mengembangkan, menjual, mendukung, dan mendistribusikan produk. Beberapa vendor mengintegrasikan produk ke dalam sistem atau layanan, dan vendor ini dapat bertindak sebagai pelanggan atau pengguna produk komponen. Vendor tersebut dapat bergantung pada vendor komponen untuk informasi remediasi kerentanan.

5.5.4 Pelapor

Pelapor melakukan notifikasi kepada vendor tentang potensi kerentanan. Pelapor biasanya, tetapi tidak selalu, menjumpai atau menemukan kerentanan. Penemuan tersebut mungkin bukan penemuan pertama atau satu-satunya. Untuk tujuan dokumen ini, diasumsikan bahwa pelapor akan berupaya menginformasikan vendor atau koordinator tentang kerentanan. Pada praktiknya, pelapor dapat memilih untuk tidak berupaya menginformasikan vendor atau koordinator, atau upaya tersebut dapat gagal. Penerimaan laporan kerentanan didiskusikan dalam Pasal 6.

Pelapor sering kali merupakan peneliti keamanan, tetapi penting untuk menegaskan bahwa setiap individu atau organisasi dapat bertindak sebagai pelapor. Peneliti professional dapat mengoperasikan secara independen atau sebagai bagian dari organisasi. Beberapa peneliti diasosiasikan dengan universitas atau institusi akademis lainnya. Pelapor lainnya tidak secara reguler melakukan analisis atau riset keamanan tetapi mengidentifikasi kerentanan dalam aktivitas lain atau bahkan secara tidak sengaja. Vendor, pengguna, dan koordinator dapat semuanya bertindak sebagai pelapor.

Keberagaman pelapor memiliki implikasi terhadap mutu laporan kerentanan dan keterbiasaan pelapor dengan praktik pengungkapan.
Pelapor terkadang khawatir dengan tekanan hukum atau tekanan lainnya yang harus mereka tanggung. Tekanan tersebut dapat menimbulkan “efek menakutkan”, mengurangi kemungkinan pelaporan.

5.5.5 Koordinator

Koordinator secara umum bertindak sebagai perantara antara pelapor dan vendor. Layanan umum yang disediakan koordinator termasuk:

— mengidentifikasi dan menghubungi vendor;

— memanajemeni kerentanan yang berdampak pada multipel vendor;

— melakukan analisis dan validasi teknis;

— menegosiasikan lini masa pengungkapan;

— mendukung pelapor;

— memublikasikan advisori;

— mengedukasi vendor dan pelapor tentang proses pengungkapan.

Koordinator tidak perlu terlibat dalam setiap pengungkapan. Untuk kasus yang melibatkan satu atau sedikit kerentanan yang berdampak pada satu vendor, seorang pelapor dan vendor sering kali sudah cukup. Koordinator dapat membantu negosiasi ketika multipel vendor terdampak, pelapor dan vendor tidak setuju, atau timbul kompleksitas lainnya.

Koordinator dapat bekerja dengan koordinator lainnya untuk memperoleh bantuan dalam domain keahlian, bahasa, geografis, dan hambatan budaya serta untuk berbagi sumber daya dan upaya. Beberapa tim tanggap insiden keamanan komputer (*Computer security incident response teams* – CSIRT) menyediakan layanan koordinasi kerentanan yang luas pada basis operasional, sementara CSIRT lainnya berkoordinasi dengan cara yang lebih terbatas, misalnya, mencakup wilayah, industri yang spesifik, atau pada basis sesuai kebutuhan.

Beberapa vendor dan pemerintah menyediakan layanan koordinasi gratis sementara beberapa vendor menawarkan layanan koordinasi komersial.

Beberapa vendor menyediakan layanan koordinasi, seperti halnya beberapa vendor keamanan komersial. Misalnya, beberapa organisasi membayar pelapor untuk melaporkan kerentanan, menggunakan informasi kerentanan tersebut untuk menyediakan proteksi komersial kepada pelanggannya, dan juga bertindak sebagai koordinator, mengungkap secara privat kepada vendor dan nantinya kepada publik. Terdapat variasi dan tingkatan penawaran koordinasi kerentanan yang berorientasi komersial.

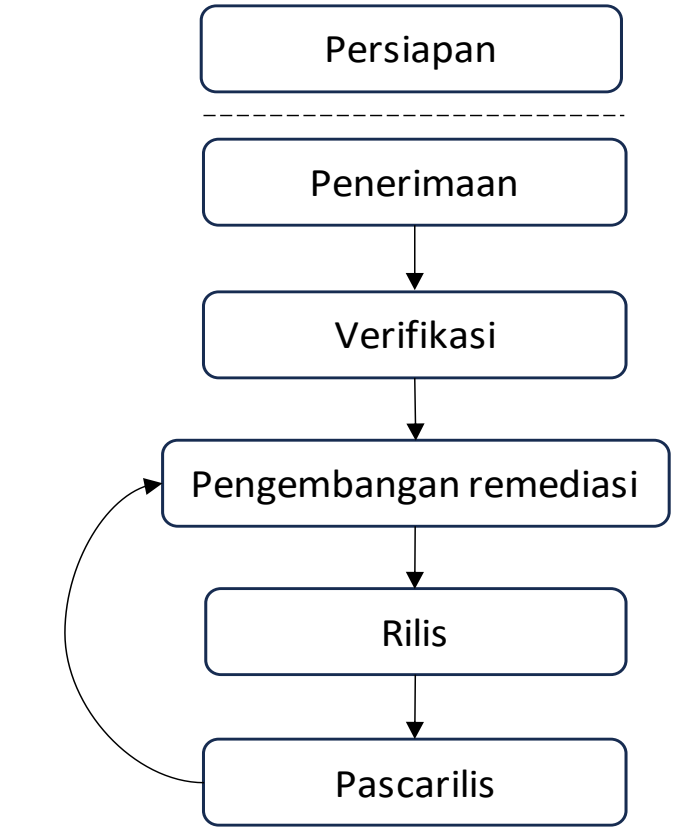
Sementara koordinator sering kali memiliki kepentingan untuk melindungi konstituennya, koordinator sebaiknya mencoba untuk objektif secara teknis dan meminimalkan risiko bagi seluruh pemangku kepentingan.

Koordinasi dideskripsikan lebih lanjut dalam Pasal 8.

5.6 Ringkasan proses penanganan kerentanan

5.6.1 Umum

Subpasal ini meringkas proses penanganan kerentanan yang dideskripsikan lebih lanjut dalam ISO/IEC 30111. Gambar 2 menguraikan proses penanganan kerentanan vendor termasuk langkah awal untuk mengembangkan kebijakan dan kapabilitas pengungkapan kerentanan.



Gambar 2 – Ringkasan proses penanganan kerentanan

5.6.2 Persiapan

Vendor sebaiknya mengembangkan kebijakan (lihat Pasal 9), proses, dan kapabilitas sebelum memulai program pengungkapan kerentanan. Persiapan dapat meliputi pembuatan organisasi tanggap (sering disebut sebagai PSIRT atau CSIRT), perekrutan dan penugasan staf, pengembangan alat, dan pemublikasian informasi tentang program.

Vendor sebaiknya mempertimbangkan untuk melakukan asesmen produk dan layanan dalam lingkup program. Asesmen tersebut dapat mengidentifikasi kerentanan yang ditemukan dengan mudah dan mengurangi jumlah laporan sebelum program dimulai.

5.6.3 Penerimaan

Pelapor mengidentifikasi potensi kerentanan dalam produk atau layanan dan memberi notifikasi vendor. Vendor menyatakan penerimaan laporan tersebut.

Jika vendor tidak dapat menerima laporan kerentanan, pelapor atau koordinator dapat memutuskan untuk memublikasikan advisori tanpa sepengetahuan vendor tersebut. Pelapor, atau siapa pun yang memiliki informasi kerentanan dapat mengungkapkan atau memublikasikan informasi tersebut kapan saja.

Penerimaan laporan kerentanan dideskripsikan dalam Pasal 6.

5.6.4 Verifikasi

Vendor menginvestigasi laporan. Investigasi sering melibatkan upaya mereproduksi lingkungan dan perilaku yang dilaporkan oleh pelapor. Ini dapat menjadi investigasi awal, difokuskan terutama pada kebutuhan upaya lebih lanjut oleh vendor. Investigasi dapat juga meliputi laporan yang serupa atau terkait, menilai tingkat keparahan, dan menentukan produk lain yang terdampak. Investigasi menentukan apakah laporan tersebut merupakan kerentanan atau bukan. Vendor dapat berkomunikasi dengan pelapor selama investigasi, dan vendor memberi tahu pelapor tentang hasilnya di akhir investigasi. Fase ini sering disebut “triase”.

5.6.5 Pengembangan remediasi

Vendor mengembangkan remediasi untuk kerentanan. Pengembangan remediasi dapat melibatkan investigasi yang lebih detail mengenai penyebab utama kerentanan dan penentuan produk lain yang terdampak dari kerentanan yang sama atau serupa. Vendor biasanya mengembangkan teknik remediasi dan mitigasi serta melakukan tes positif untuk menentukan bahwa remediasi bekerja dengan benar, dan tes negatif (regresi) untuk menyediakan kepastian bahwa remediasi tidak mengganggu fungsionalitas yang sudah ada.

Vendor sebaiknya memasukkan kembali informasi tentang kerentanan dan analisis penyebab utama ke dalam siklus hidup pengembangan atau pedoman penggelaran perangkat lunak, untuk menghindari timbulnya tipe kerentanan yang sama di masa depan. Lihat juga ISO/IEC 27034-1[4].

5.6.6 Rilis

Vendor mengembangkan dan mendistribusikan remediasi dengan aman. Untuk sebuah produk, vendor menyediakan informasi remediasi dan mitigasi kepada pengguna, biasanya dalam bentuk advisori kerentanan dan *patch* atau pembaruan perangkat lunak, dan pengguna menerapkan remediasi tersebut.

Untuk kerentananan layanan, vendor menggelar remediasi dan secara opsional mengungkapkan kerentanan tersebut.

Vendor dapat merilis advisori sebelum remediasi tersedia, khususnya dalam kasus eksploitasi aktif atau diskusi publik. Vendor sebaiknya berupaya memastikan remediasi tidak menimbulkan kerentanan baru, masalah mutu produk secara keseluruhan, atau memiliki masalah kompatibilitas dengan produk atau layanan lain jika memungkinkan.

Alasan penting untuk menginformasikan pengguna tentang kerentanan adalah karena pengguna sering kali perlu mengambil tindakan untuk meremediasi dan menilai ulang risiko mereka. Ketika meremediasi kerentanan dalam layanan, pengguna mungkin tidak perlu mengambil tindakan apa pun. Meskipun demikian, ada alasan lain untuk memublikasikan informasi kerentanan, meliputi:

— dukungan untuk investigasi insiden atau forensik, mengetahui kapan adanya kerentanan (dan tidak diremediasi);

— meningkatkan praktik desain, perekayasaan, dan pengembangan yang aman;

— transparansi dan akuntabilitas, menginformasikan pengguna dan pemangku kepentingan lainnya bahwa kerentanan telah diidentifikasi dan diremediasi;

— kepastian, menginformasikan pengguna tentang nonkerentanan;

— menyediakan informasi otoritatif, disambiguasi, klarifikasi;

— menginformasikan keputusan kebijakan publik;

— mendokumentasikan perubahan sistem untuk keperluan pengembangan dan operasional;

— menyediakan pengakuan dan penghargaan kepada pelapor.

Dengan mempertimbangkan alasan di luar kebutuhan tindakan pengguna, layanan masih dapat memilih untuk memublikasikan informasi kerentanan.
Pemublikasian advisori kerentanan dideskripsikan dalam Pasal 7.

5.6.7 Pascarilis

Vendor mengumpulkan umpan balik dari pengguna dan memperbarui informasi remediasi dan mitigasi sesuai kebutuhan. Misalnya, remediasi dapat ditemukan dalam kondisi tidak lengkap atau menyebabkan masalah regresi atau efek samping.

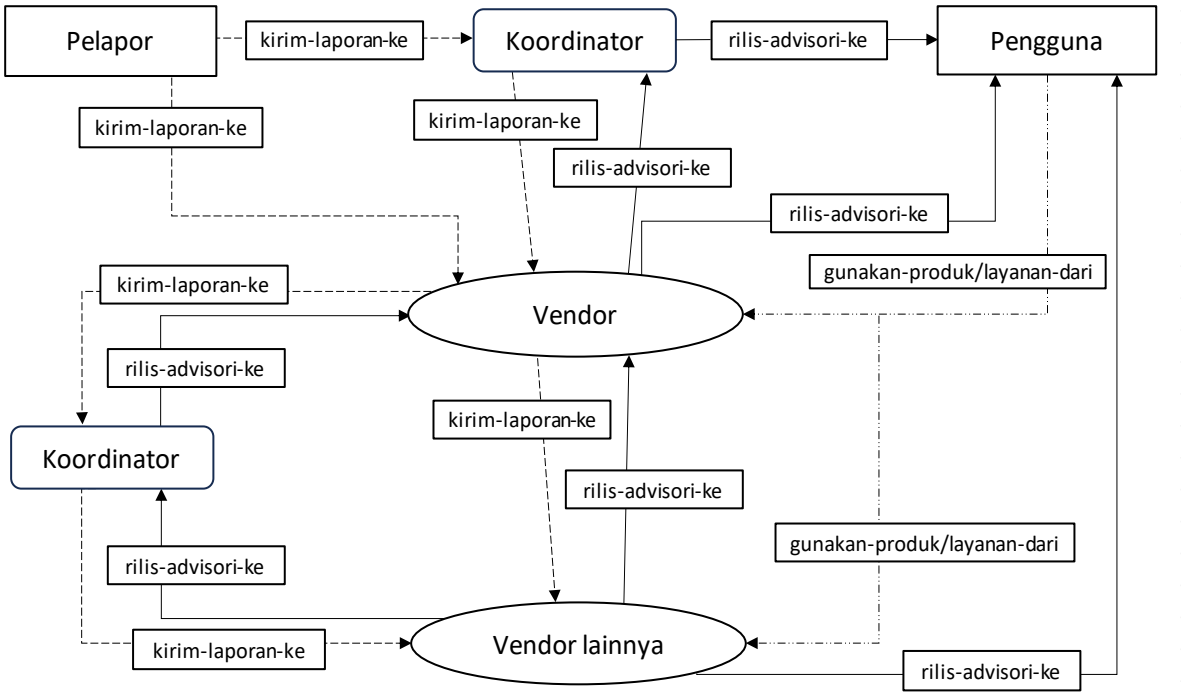
5.6.8 Periode embargo

Untuk memberikan vendor waktu untuk mengembangkan remediasi tanpa penyerang juga memiliki akses ke informasi kerentanan publik, pelapor sering kali memberi tahu vendor secara privat dan tidak mengungkapkan secara publik sampai remediasi siap atau periode embargo telah berlalu. Fase penerimaan, verifikasi, dan pengembangan remediasi biasanya tercakup dalam periode embargo. Pelapor dan pihak lain yang mengetahui kerentanan memiliki kemampuan untuk mengungkap secara publik kapan saja. Pelapor menggunakan periode embargo berbeda, yang terkadang dapat dinegosiasikan.

5.7 Pertukaran informasi selama pengungkapan kerentanan

Gambar 3 mengilustrasikan pertukaran informasi selama pengungkapan kerentanan. Terdapat dua pertukaran utama: Laporan potensi kerentanan dari pelapor kepada vendor, dan advisori dari vendor kepada pengguna. Laporan potensi kerentanan dikirim dari pelapor kepada vendor baik secara langsung atau melalui koordinator. Vendor dapat bertindak sebagai pelapor dan melaporkan kerentanan kepada vendor lain. Advisori dirilis oleh vendor baik secara privat kepada penggunanya atau, secara lebih umum, kepada publik. Dokumen ini berfokus pada kedua pertukaran dari perspektif vendor yang menerima laporan kerentanan dan memublikasikan informasi remediasi.

Proses pengungkapan kerentanan yang lengkap dapat meliputi multipel peristiwa pengungkapan, seperti pelapor melaporkan kepada vendor, vendor memublikasikan advisori, atau koordinator memberi tahu vendor lainnya.



Gambar 3 — Pertukaran informasi kerentanan

5.8 Konfidensialitas informasi yang ditukar

5.8.1 Umum

Karena informasi kerentanan dapat digunakan untuk menyerang sistem yang rentan, informasi kerentanan yang sensitif sebaiknya dikomunikasikan secara rahasia, terutama ketika informasi tersebut tidak tersedia secara publik.

5.8.2 Komunikasi yang aman

Vendor sebaiknya menyediakan metode konfidensial yang aman bagi pelapor untuk melaporkan informasi kerentanan. Integritas pesan juga penting, terutama dalam memverifikasi bahwa informasi remediasi tersebut autentik. Protokol dan implementasi kriptografi yang umum seperti TLS, S/MIME, dan OpenPGP dapat menyediakan konfidensialitas dan integritas. Jika terdapat persyaratan keamanan lainnya, ISO/IEC 27010[2] dapat menjadi relevan. Contohnya jika koordinator menawarkan layanan anonimitas kepada pelapor.

5.9 Advisori kerentanan

Informasi kerentanan secara umum dipublikasikan di dalam advisori. Advisori tersebut yang mendeskripsikan kerentanan, biasanya berfokus pada remediasi dan mitigasi, tetapi dapat juga termasuk informasi tentang sistem yang terdampak, ancaman, dampak, dan referensi.
Pengguna yang membaca advisori membutuhkan informasi yang cukup untuk membuat

keputusan risiko yang terinformasi tentang bagaimana meremediasi atau memitigasi kerentanan.

Pemublikasian advisori kerentanan dideskripsikan dalam Pasal 7.

5.10 Eksploitasi kerentanan

Secara umum, penyerang berusaha mengeksploitasi kerentanan untuk mendapatkan keuntungan, hampir selalu menyebabkan kerugian bagi pengguna. Berbagai faktor seperti populasi target, eksposur target, nilai target bagi penyerang, dan biaya pengembangan eksploitasi, dapat memengaruhi apakah suatu kerentanan akan dieksploitasi atau tidak oleh penyerang. Namun, setiap upaya untuk memprediksi apakah kerentanan akan atau telah digunakan dalam serangan dapat menghadapi ketidakpastian yang cukup besar. Asumsi yang paling konservatif adalah kerentanan dapat dan akan (dan mungkin sudah) digunakan dalam serangan.

5.11 Kerentanan dan risiko

Kerentanan berkontribusi terhadap risiko, terutama ketika dieksploitasi serangan. Pengungkapan kerentanan menginformasikan pemangku kepentingan tentang kerentanan dan idealnya termasuk informasi remediasi, yang mengarah pada perbaikan kerentanan dan pengurangan risiko. Pengungkapan kerentanan itu sendiri menciptakan risiko, karena pengungkapan publik menyediakan informasi bagi developer eksploit dan penyerang. Teori yang mendukung pengungkapan kerentanan menyatakan bahwa risiko jangka pendek yang disebabkan pengungkapan publik tidak sebanding dengan keuntungan jangka panjang dari perbaikan kerentanan, defender yang memiliki informasi lebih baik, dan peningkatan defensif sistemis.

6 Penerimaan laporan kerentanan

6.1 Umum

Pasal ini menyediakan panduan bagi vendor dalam menerima informasi tentang potensi kerentanan. Kapabilitas dalam menerima laporan kerentanan membantu vendor lebih cepat mengetahui laporan baru dan membentuk hubungan kerja dengan pelapor dan pemangku kepentingan lainnya.

6.2 Laporan kerentanan

6.2.1 Umum

Pelapor menotifikasi vendor tentang potensi kerentanan. Laporan biasanya mencakup deskripsi produk atau layanan yang terdampak, bagaimana potensi kerentanan tersebut dapat diidentifikasi, ditunjukkan, atau direproduksi, dan tipe dampak fungsional yang disebabkan oleh kerentanan tersebut.

Laporan mencakup kode pembuktian konsep (*proof-of-concept* – PoC) yang menunjukkan eksploitasi kerentanan. Karena laporan kerentanan umumnya mengandung informasi sensitif, nonpublik, vendor sebaiknya menyediakan mekanisme untuk menerima laporan secara konfidensial (lihat 5.8 dan 6.7).

6.2.2 Kapabilitas untuk menerima laporan

Vendor harus menyediakan satu atau beberapa mekanisme yang secara teknis terkini dan

dapat digunakan untuk menerima laporan potensi kerentanan. Hal ini sesuai dengan fase penerimaan yang dideskripsikan pada 5.6.3.

Mekanisme pelaporan biasanya termasuk:

— formulir web;

— sistem pelacakan bug atau masalah;

— layanan pelaporan kerentanan;

— surel, yang mungkin alamat nama alias samaran, lis, atau peran yang tidak bergantung pada individu mana pun.

Vendor sebaiknya memilih mekanisme yang aman untuk menerima laporan, tetapi mungkin menerima laporan melalui mekanisme yang kurang aman seperti surel teks terang atau sistem pelacakan *bug* publik.

Untuk memfasilitasi langkah verifikasi proses penanganan kerentanan, vendor sebaiknya merancang mekanisme pelaporan untuk mendapatkan informasi yang berguna dalam menilai validitas, tingkat keparahan, ruang lingkup, dan dampak kerentanan. Informasi tersebut termasuk:

— nama produk atau layanan dan versi yang terdampak;

— kelas atau tipe kerentanan, secara opsional menggunakan taksonomi seperti CWE;

— kemungkinan penyebab utama;

— kode PoC atau bukti substansial lainnya;

— alat dan langkah untuk mereproduksi perilaku yang rentan;

— perkiraan dampak dan tingkat keparahan;

— asesmen ruang lingkup, produk lain, komponen, layanan, atau vendor lain yang dianggap terdampak;

— rencana pengungkapan, secara spesifik lini masa embargo dan publikasi.

Untuk contoh lebih lanjut tentang informasi yang perlu diminta dalam sebuah laporan, lihat Lampiran B.

6.2.3 Monitoring

Vendor harus memonitor mekanisme pelaporan mereka untuk laporan dan komunikasi baru yang berkaitan dengan laporan yang sudah ada. Sebagai tambahan, vendor sebaiknya memonitor sumber publik (termasuk milis dan media sosial yang digunakan oleh komunitas riset keamanan) untuk laporan kerentanan. Vendor juga sebaiknya memonitor layanan dan dukungan pelanggan serta kanal komunikasi organisasi lainnya yang kemungkinan menerima laporan kerentanan.

6.2.4 Pelacakan laporan

Vendor sebaiknya menggunakan mekanisme untuk melabeli (menugaskan pengidentifikasi)

dan melacak laporan, misalnya, pelacakan bug, CRM, atau sistem tiket. Vendor sebaiknya menyediakan pengidentifikasi laporan kerentanan kepada pelapor dan pemangku kepentingan lainnya. Vendor dapat menggunakan lebih dari satu mekanisme pelabelan dan pelacakan, namun mekanisme multipel dapat menyebabkan kebingungan.

Pemangku kepentingan lainnya dapat juga menggunakan mekanisme pelabelan dan pelacakan.

6.2.5 Pengakuan laporan

Vendor harus mengakui penerimaan laporan potensi kerentanan dalam 7 hari kalender.

Respons dapat dilakukan secara otomatis, tetapi sebaiknya dapat dipahami. Respons sebaiknya mencakup nomor pelacakan atau pengidentifikasi, dan informasi status awal. Respons dapat mengindikasikan bahwa laporan tersebut sedang diinvestigasi, atau mensyaratkan informasi lebih lanjut, atau dianggap tidak lengkap, palsu, atau sebaliknya tidak relevan.

Dalam kasus laporan yang sangat tidak akurat, berulang, atau palsu, tidak diperlukan respons dan respons otomatis dapat diterima.

Pengakuan awal dari vendor kepada pelapor penting dalam membentuk hubungan kerja. Banyak pelapor yang menjadi frustasi karena ketidakmampuan untuk melapor kepada vendor atau kurangnya respons dari vendor. Pelapor yang frustasi lebih cenderung mencari cara lain untuk melakukan pengungkapan, termasuk pengungkapan publik[14].

Sebagian besar proses pengembangan remediasi tidak terlihat oleh pelapor. Oleh karena itu penting untuk mengomunikasikan ekspektasi realistis dan pembaruan status kepada pelapor.

6.3 Asesmen awal

Vendor harus melakukan asesmen awal, atau triase, terhadap laporan kerentanan. Hal ini sesuai dengan fase Verifikasi yang dideskripsikan pada 5.6.4. Laporan dapat diprioritaskan dan dikategorikan berdasarkan tingkat keparahan, dampak, ruang lingkup, kemudahan eksploitasi, kemungkinan penemuan secara independen, dan faktor lainnya.

Fase asesmen awal ini dapat membosankan dan memakan waktu. Laporan baru harus diperiksa dengan cukup hati-hati untuk meminimalkan negatif palsu. Artinya, asesmen awal harus dirancang untuk mempunyai sensitivitas tinggi, mengidentifikasi dan menolak laporan yang bukan merupakan kerentanan dengan benar, dengan mengorbankan penerimaan laporan yang nantinya berubah menjadi bukan kerentanan. Laporan baru juga harus dikomparasikan dengan laporan yang sudah ada untuk mengidentifikasi duplikasi.

Pada fase ini, vendor sebaiknya memperhatikan secara signifikan untuk hanya menolak laporan yang dianggap kuat bukan kerentanan dan tidak membutuhkan respons lebih lanjut. Dalam kasus seperti ini, pelapor harus diberi informasi tentang asesmen vendor.

Jika vendor tidak menganggap laporan sebagai kerentanan, vendor harus menginformasikan pelapor dan pemangku kepentingan lainnya.

6.4 Investigasi lebih lanjut

Untuk laporan yang mensyaratkan investigasi lebih lanjut atau dianggap sebagai kerentanan yang valid, vendor harus memulai proses penanganan kerentanan. Seperti disebutkan dalam Gambar 1, proses tersebut dideskripsikan dalam ISO/IEC 30111. Investigasi dan penanganan

kerentanan sesuai dengan fase pengembangan remediasi yang dideskripsikan pada 5.6.5.

Untuk melakukan investigasi lebih lanjut, vendor dapat berkomunikasi dengan pelapor dan pemangku kepentingan internal dan eksternal lainnya untuk memahami kerentanan dan dampaknya. Vendor sebaiknya meminta informasi tambahan dari pelapor sesuai kebutuhan untuk sepenuhnya menilai atau mereproduksi kerentanan yang dilaporkan.

Jika vendor lain terdampak atau kemungkinan akan terdampak, vendor awal sebaiknya memberi tahu vendor lainnya atau melibatkan koordinator. Vendor harus mengetahui hubungan rantai pasokan dan penggunaaan umum komponen bersama atau serupa, seperti pustaka, protokol, dan format.

6.5 Komunikasi yang sedang berlangsung

Selama penanganan kerentanan, vendor harus berkomunikasi dengan pelapor dan pemangku kepentingan lainnya. Komunikasi tersebut sebaiknya mencakup informasi seperti:

— pembaruan status;

— informasi baru yang signifikan;

— perubahan pada rencana yang ada;

— pengaturan waktu pengungkapan.

Ketika terdapat ketidaksepakatan di antara pemangku kepentingan, terutama mengenai pengungkapan publik, vendor sebaiknya mengomunikasikan intensi mereka sehingga para pemangku kepentingan tidak terkejut.

Hubungan rantai pasokan, atau kebutuhan untuk melibatkan pemangku kepentingan lainnya selama investigasi, dapat menyebabkan penundaan tambahan pada komunikasi. Jika diperlukan, vendor sebaiknya menjelaskan penundaan komunikasi dan proses kepada pemangku kepentingan.

6.6 Keterlibatan koordinator

Koordinator dapat dilibatkan dalam fase penerimaan. Koordinator dapat bertindak sebagai pelapor, atau atas nama pelapor, yang berupaya untuk mengidentifikasi dan melaporkan kerentanan kepada vendor. Koordinator dapat memediasikan antara pelapor dan vendor.

Koordinator juga dapat menyediakan dukungan tambahan dalam menilai validitas, tingkat keparahan, dampak, dan ruang lingkup kerentanan.
Koordinasi dideskripsikan lebih lanjut dalam Pasal 8.

6.7 Keamanan operasional

Vendor sebaiknya mempertimbangkan keamanan operasional selama proses penerimaan dan komunikasi tentang laporan kerentanan.

Mekanisme pelaporan (lihat 6.2) dan komunikasi yang sedang berlangsung (lihat 6.5) sebaiknya menyediakan konfidensialitas untuk membatasi akses terhadap informasi kerentanan nonpublik yang sensitif. Mekanisme pelaporan dan komunikasi dapat juga menyediakan autentikasi. Mekanisme pelaporan sebaiknya menyediakan pelapor kemampuan untuk memverifikasi identitas vendor.

Mekanisme keamanan biasanya termasuk:

— formulir atau aplikasi berbasis web menggunakan TLS (HTTPS);

— enkripsi dan penandatanganan surel menggunakan S/MIME atau OpenPGP.

Vendor sebaiknya mempertimbangkan keamanan operasional internal dan membatasi akses informasi kerentanan nonpublik hanya kepada staf dan unit organisasi yang perlu mengetahui.

7 Pemublikasian advisori kerentanan

7.1 Umum

Pasal ini menyediakan panduan dalam mengungkapkan informasi kerentanan kepada pengguna, pemangku kepentingan lainnya, dan publik. Pada sebagian besar kasus, pada fase ini vendor telah mengembangkan dan mengetes remediasi untuk kerentanan, sudah mengikuti proses yang dideskripsikan dalam ISO/IEC 30111. Pada sebagian besar kasus, vendor sebaiknya memublikasikan, atau mengungkap secara publik, informasi tentang pengidentifikasian dan peremediasian kerentanan. Pemublikasian advisori secara umum sesuai dengan fase Rilis yang dideskripsikan pada 5.6.6.

7.2 Advisori

Istilah advisori digunakan secara luas untuk mengartikan setiap dokumen atau pesan yang berisi informasi kerentanan. Advisori harus diintensikan untuk penyebarluasan, biasanya pengungkapan publik (publikasi) dan sebaiknya memungkinkan pengguna untuk mengidentifikasi produk dan layanan yang rentan serta mengambil tindakan untuk meremediasi kerentanan. Penulis advisori sebaiknya mempertimbangkan kebutuhan audiens yang dituju dan membuat advisori yang efektif dalam hal konten informatif, mekanisme distribusi, dan format presentasi.

Contoh advisori dapat ditemukan dalam Lampiran C.

7.3 Pengaturan waktu publikasi advisori

Vendor sebaiknya berupaya untuk menyeimbangkan risiko ketika memilih kapan akan memublikasikan advisori. Untuk mengurangi gangguan terhadap pengguna, vendor dapat memublikasikan advisori perkelompok dan menjadwalkan perilisan terlebih dahulu. Vendor juga dapat memublikasikan advisori secepatnya setelah remediasi terkait tersedia.

Jika kerentanan sedang tereksploitasi secara aktif dan remediasi tidak tersedia, vendor sebaiknya memublikasikan advisori yang menginformasikan pengguna tentang ancaman saat ini dan langkah apa yang dapat diambil oleh pengguna untuk mengurangi risiko sampai remediasi tersedia.

Vendor sebaiknya, ketika memungkinkan, berupaya untuk mengoordinasikan perilisan advisori ketika produk mereka terdampak kerentanan yang saling terkait. Perilisan informasi tentang kerentanan pada satu produk dapat mengekspos produk interdependen lain terhadap risiko serangan yang meningkat. Situasi ini biasanya terjadi ketika pustaka, protokol, modul atau komponen lain pada perangkat lunak digunakan dalam multipel produk atau layanan, yang sering kali berdampak pada multipel vendor. Ada kemungkinan bahwa koordinator dapat memfasilitasi pengaturan waktu pengungkapan dan publikasi advisori di antara multipel vendor.

Faktor lain yang perlu dipertimbangkan termasuk:

— setiap periode embargo (lihat 5.6.8);

— perkiraan waktu antara publikasi dan remediasi diaplikasikan (lihat 5.6.6);

— agenda pelapor untuk publikasi;

— jadwal perilisan advisori vendor lainnya;

— kemungkinan efek samping negatif dari solusi atau remediasi;

— lokalisasi bahasa;

— kesiapan remediasi untuk versi atau platform berbeda;

— kesiapan dukungan pelanggan dan organisasi penjualan.

7.4 Elemen advisori

7.4.1 Umum

Advisori sebaiknya berisi informasi yang cukup untuk memungkinkan audiens target — termasuk administrator sistem, developer, manajer, dan pengguna — untuk memutuskan apakah kerentanan tersebut relevan dan bagaimana cara meremediasinya.

Pembaca advisori memiliki kebutuhan berbeda yang dapat dependen terhadap segmen pasar atau persyaratan regulasi. Pengguna teknis seperti administrator sistem cenderung lebih memilih informasi yang detail tentang kerentanan dan solusi. Konsumen biasanya menghargai informasi tentang bagaimana menentukan apakah mereka menggunakan produk terdampak dan saran remediasi yang jelas dan mudah dipahami. Vendor sebaiknya merancang advisori untuk audiens yang dituju. Satu advisori dapat mengatasi banyak kerentanan, misalnya, ketika satu remediasi menyelesaikan multipel kerentanan.

Subpasal berikut ini mendeskripsikan elemen yang termasuk dalam advisori. Daftar ini tidak mendalam dan vendor mungkin menyertakan elemen tambahan. Kecuali dinyatakan lain, urutan subpasal ini tidak mengindikasikan urutan elemen yang muncul dalam suatu advisori.

7.4.2 Pengidentifikasi

Advisori harus berisi pengidentifikasi tertentu.

a) Pengidentifikasi advisori: Suatu advisori harus dilabeli dengan pengidentifikasi yang unik dan konsisten untuk dokumen advisori. Pengidentifikasi CVE dapat digunakan sebagai pengidentifikasi advisori jika satu advisori mendeskripsikan hanya satu kerentanan. Sebisa mungkin pengidentifikasi CVE ditetapkan untuk kerentanan individu. Satu advisori dapat mengatasi multipel kerentanan.

b) Pengidentifikasi kerentanan: Suatu advisori harus menyediakan pengidentifikasi yang unik dan konsisten untuk kerentanan yang dituju dalam advisori. Pengidentifikasi harus cukup unik dan konsisten sehingga tidak menyebabkan kebingungan pada advisori dan kerentanan yang berbeda. Penulis advisori sebaiknya memilih sistem identifikasi kerentanan bersama yang umum seperti CVE.

c) Pengidentifikasi produk: Suatu advisori harus menyertakan nama dan informasi versi produk untuk menginformasikan pembaca tentang produk mana yang terdampak dan secara opsional produk mana yang tidak terdampak. Lihat 7.4.6.

7.4.3 Tanggal dan waktu

Advisori harus mengindikasikan tanggal publikasi awal dan mungkin menyertakan tanggal lainnya, misalnya, sebagai bagian dari riwayat revisi. Advisori harus menggunakan referensi tanggal dan waktu yang takambigu dan menggunakan ISO 8601[8].

7.4.4 Judul

Judul advisori sebaiknya berisi referensi pada suatu produk atau beberapa deskripsi lain yang informatif bagi pembaca sehingga mereka dapat memutuskan secara cepat apakah advisori tersebut relevan.

7.4.5 Ikhtisar

Elemen ikhtisar menyediakan ringkasan kerentanan yang singkat dan berlevel tinggi sehingga pengguna dapat memahami poin penting laporan dan secara cepat menentukan apakah advisori tersebut dapat diterapkan pada lingkungan mereka.

7.4.6 Produk terdampak

Advisori harus menyediakan informasi yang cukup bagi pengguna untuk menentukan apakah mereka terdampak oleh kerentanan atau tidak.

Elemen advisori ini menyediakan daftar produk dan versinya yang diketahui, didukung, dan terdampak. Elemen ini dapat menyediakan instruksi tentang bagaimana cara memverifikasi versi produk tersebut. Dalam sebagian besar kasus, layanan tidak memiliki pengidentifikasi versi tetapi dapat memiliki tanggal kapan pembaruan atau perubahan terakhir dilakukan.

Elemen ini dapat secara opsional mencatat produk dan versi yang tidak lagi didukung atau takterdampak kerentanan.

Informasi yang berguna dalam mendeskripsikan produk yang terdampak dapat termasuk:

— nama produk, termasuk nama-nama umum atau historis;

— nomor versi atau *string*;

— *hash* berkas;

— kode PoC untuk mengetes keberadaan kerentanan secara aman.

7.4.7 Audiens yang dituju

Penulis advisori sebaiknya mempertimbangkan audiens yang dituju mereka ketika mengembangkan dan memproduksi advisori. Biasanya, audiens adalah pengguna yang bertanggung jawab mengidentifikasi sistem yang rentan dan melakukan remediasi. Advisori dapat menyediakan bagian yang ditujukan kepada audiens spesifik, misalnya, saran remediasi yang berbeda untuk developer, administrator sistem, atau pengguna akhir. Bahasa khusus audiens dalam advisori bersifat opsional.

7.4.8 Lokalisasi

Vendor dapat menyediakan advisori dengan pilihan bahasa dan lokalisasi yang sesuai.

7.4.9 Deskripsi

Advisori sebaiknya menyediakan informasi yang cukup sehingga pengguna dapat mengetahui apakah mereka terdampak dan menilai eksposur mereka. Pada saat yang sama advisori sebaiknya tidak menyediakan terlalu banyak detail untuk menghindari eksploitasi kerentanan menjadi lebih mudah.

Advisori dapat mendeskripsikan kelas atau tipe kerentanan, misalnya menggunakan taksonomi CWE.

7.4.10 Dampak

Advisori sebaiknya mendeskripsikan potensi dampak atau konsekuensi kerentanan jika terekploitasi. Dampak tersebut minimal menjelaskan perilaku teknis langsung yang dimungkinkan oleh kerentanan. Dampak tersebut dapat mendeskripsikan pelanggaran keamanan, perolehan hak akses atau hak istimewa, kemungkinan dampak selanjutnya, dan skenario serangan yang umum.

Dampak dapat dideskripsikan menggunakan model seperti *CIA triad* (konfidensialitas, integritas, dan availabilitas) atau *Parkerian hexad* (konfidensialitas, kepemilikan atau kontrol, integritas, autentisitas, availabilitas, dan utilitas).

7.4.11 Tingkat keparahan

Advisori sebaiknya menyediakan tingkat keparahan pada setiap kerentanan untuk membantu pengguna menilai risiko lebih cepat dan terprogram. Penulis advisori sebaiknya mempertimbangkan sistem yang sudah ada seperti CVVS, tetapi dapat menggunakan sistem lain atau yang mengembangkan sistem sendiri. Sistem rating tingkat keparahan yang digunakan dalam advisori harus didokumentasikan dan dokumentasinya direferensikan dari advisori.

7.4.12 Remediasi

Advisori sebaiknya menyediakan informasi mengenai tindakan apa yang harus diambil pengguna yang terdampak untuk meremediasi kerentanan dan mengurangi dampaknya. Remediasi biasanya melibatkan instalasi pemutakhiran (*upgrade*), *patch*, atau versi baru.
Jika sesuai atau diperlukan, advisori sebaiknya menyediakan solusi sementara (*workaround*) yang dapat digunakan pengguna untuk melindungi produk atau layanan terdampak hingga solusi yang lebih permanen diimplementasikan. Solusi sementara dapat termasuk mengubah konfigurasi produk untuk membatasi fungsionalitas dan menerapkan tembok api (*firewall*) untuk membatasi aksesibilitas jaringan.

7.4.13 Referensi

Referensi atas informasi tambahan atau terkait dapat ditambahkan pada elemen ini. Contoh referensi tersebut dapat berupa tautan ke advisori terkait yang dipublikasikan oleh pihak lain atau referensi ke pengidentifikasi CVE. Penting untuk merujuk pada materi asli atau sumber dan referensi silang yang umum seperti CVE.

7.4.14 Kredit

Pada elemen ini, vendor sebaiknya mengakui pelapor karena telah melaporkan kerentanan dan kooperatif selama proses tersebut, jika pelapor ingin diberi kredit secara publik. Ini adalah elemen opsional.

7.4.15 Informasi kontak

Advisori sebaiknya menyediakan informasi kontak sehingga pembaca advisori dapat mengontak vendor.

7.4.16 Riwayat revisi

Elemen ini sebaiknya berisi tanggal advisori pertama kali dipublikasikan. Ini mungkin berisi riwayat modifikasi jika advisori selanjutnya diperbarui.

7.4.17 Ketentuan penggunaan

Advisori sebaiknya menyediakan informasi tentang hak cipta dan ketentuan penggunaan serta redistribusi advisori.

7.5 Komunikasi advisori

Vendor sebaiknya membuat dan memelihara metode yang sesuai untuk mengomunikasikan advisori kepada penggunanya. Metode yang umum termasuk situs web, milis, *feeds*, dan mekanisme pembaruan otomatis. Setiap vendor dapat menentukan metode terbaik yang berlaku untuk komunitas penggunanya. Vendor juga dapat memilih untuk mengunggah advisori ke forum diskusi kerentanan publik untuk membagikan informasi mereka dengan audiens yang lebih luas.

Basis data kerentanan memonitor pengungkapan publik dan mengumpulkan laporan kerentanan. Pengontakan basis data secara langsung, pengungkapan dalam forum yang termonitor, atau penyediaan kanal distribusi yang stabil dan konsisten dapat mengarahkan inklusi di dalam basis data kerentanan.

7.6 Format advisori

Advisori harus diformat secara konsisten dan dalam cara menyampaikan informasi penting yang jelas. Perubahan pada format kemungkinan akan mensyaratkan pembaca untuk mengubah alat dan proses yang digunakan untuk menggunakan advisori. Oleh
karena itu, perubahan sebaiknya tidak sering dilakukan.

Penulis advisori sebaiknya mempertimbangkan untuk menyediakan konten pada format yang dapat dibaca oleh manusia dan mesin, seperti CVRF. Format advisori yang bisa dibaca mesin harus didokumentasikan.

7.7 Autentisitas advisori

Vendor harus menyediakan kemampuan untuk mengautentikasi dan memverifikasi integritas advisori. Hal ini dapat dicapai dengan menandatangani advisori secara kriptografi. Menerima advisori palsu dan menindaklanjutinya dapat menyebabkan sistem dapat dibobol. Bergantung pada teknik kriptografi yang digunakan, vendor sebaiknya memublikasikan materi atau kredensial kriptografi yang disyaratkan (misalnya kunci atau sertifikat publik).

7.8 Remediasi

7.8.1 Umum

Tujuan utama advisori adalah untuk mendokumentasikan remediasi (lihat 7.4.10). Advisori dapat mendeskripsikan aktivitas remediasi. Remediasi sering kali dalam bentuk perubahan perangkat lunak.

7.8.2 Autentisitas remediasi

Jika pengguna disyaratkan mengambil tindakan untuk mengaplikasikan remediasi, maka vendor harus menyediakan kemampuan untuk mengautentikasi dan memverifikasi integritas remediasi. Biasanya, ini diimplementasikan sebagai tanda tangan digital dari pembaruan perangkat lunak.

7.8.3 Penerapan remediasi

Mekanisme yang digunakan untuk menerapkan remediasi sebaiknya disesuaikan dengan kebutuhan pengguna dan cara produk dioperasikan di lapangan. Vendor sebaiknya mempertimbangkan untuk menyediakan sistem penerapan pembaruan otomatis yang mensyaratkan interaksi pengguna yang terbatas atau tanpa interaksi pengguna. Vendor sebaiknya menyediakan metode untuk mengontrol sistem penerapan pembaruan otomatis jika sesuai. Penerapan remediasi sesuai dengan fase Rilis yang dideskripsikan pada 5.6.6.

8 Koordinasi

8.1 Umum

Koordinator dapat memainkan multipel peran dalam pengungkapan kerentanan, misalnya:

— bertindak sebagai penghubung yang terpercaya antara pihak-pihak yang terlibat;

— mengoordinasikan tanggal rilis advisori publik;

— memberdayakan komunikasi antara pemangku kepentingan utama (vendor dan pelapor);

— memberdayakan pengungkapan yang terkontrol kepada pemangku kepentingan lainnya (seperti CSIRT);

— menyediakan pengalaman dan panduan untuk proses pengungkapan;

— menyediakan keahlian spesifik-domain;

— mendukung dan memfasilitasi kolaborasi antara para pemangku kepentingan.

Koordinator sebaiknya mengatur ekspektasi yang sesuai tentang layanan dan level dukungan yang mereka berikan. Pilihan koordinator dapat bergantung pada faktor – faktor seperti kedekatan geografis, bahasa dan model operasi yang dapat diterima.

Dalam kasus ketika terdapat multipel vendor yang terdampak kerentanan, vendor sebaiknya mencoba untuk mengoordinasikan pengaturan waktu rilis advisori mereka, baik secara langsung atau dengan bantuan koordinator. Vendor dapat meminta koordinator untuk menyediakan atau memperoleh pengidentifikasi CVE. Dalam beberapa kasus, lebih dari satu koordinator dapat dilibatkan. Vendor dapat menyarankan agar seorang koordinator bertindak

sebagai pemimpin untuk mengurangi kompleksitas dan kebingungan.

8.2 Vendor yang memainkan multipel peran

8.2.1 Umum

Setelah menginvestigasi kerentanan yang dilaporkan, vendor dapat menemukan kebutuhan untuk bertindak sebagai koordinator, pelapor, atau keduanya. Jika kerentanan disebabkan oleh beberapa komponen atau platform dasar yang dipasok oleh vendor lain, vendor awal dapat bertindak sebagai pelapor atau koordinator. Sebagai tambahan, vendor terkadang menghadapi situasi di mana mereka sebaiknya melaporkan kerentanan kepada vendor lainnya, menyebabkan mereka bertindak sebagai pelapor kerentanan. Subpasal ini mendeskripsikan bagaimana laporan kerentanan harus dilakukan di antara vendor.

8.2.2 Pelaporan kerentanan di antara vendor

Kasus yang umum ketika vendor dapat melaporkan informasi kerentanan kepada vendor lainnya termasuk:

— ketika vendor yakin bahwa kerentanan pada produk atau layanan mereka disebabkan oleh komponen atau alat yang mereka izinkan untuk digunakan oleh vendor kedua;

— ketika kerentanan diidentifikasikan dengan metodologi atau wawasan baru serta banyak produk dan layanan vendor lainnya dalam kategori yang sama juga diyakini rentan; atau

— ketika kerentanan diidentifikasi dalam protokol atau format yang didukung oleh produk atau layanan vendor lain.

Vendor, pelapor, atau koordinator mungkin tidak selalu dapat mengidentifikasi semua vendor lain yang terdampak. Bahkan dalam kasus dimana vendor dapat diidentifikasi, titik poin yang tepat mungkin tidak dapat diidentifikasi. Kasus seperti itu dapat memperoleh manfaat dari keterlibatan koordinator yang dapat menyediakan dukungan tambahan pada upaya notifikasi dan kontak vendor.

8.2.3 Pelaporan informasi kerentanan kepada vendor lain

Vendor dapat melaporkan informasi kerentanan kepada vendor lain secara langsung atau tidak langsung melalui koordinator dengan cara yang sama seperti pelapor melaporkan potensi kerentanan kepada vendor. Pada kasus ini, vendor awal juga dapat menginformasikan vendor lain ketika kerentanan tersebut berkaitan dengan produk atau layanan vendor awal dan meminta vendor lain tersebut menyediakan remediasi sebelum pengungkapan publik sehingga semua vendor yang terlibat dapat menyinkronkan pengungkapan.

9 Kebijakan pengungkapan kerentanan

9.1 Umum

Untuk menyampaikan intensi dan ekspektasi, vendor harus mengembangkan dan memublikasikan kebijakan pengungkapan kerentanan eksternal. Sebagai alternatif, vendor boleh mengacu dan mematuhi kebijakan yang ada yang telah dipublikasikan. Kebijakan harus memuat unsur yang disyaratkan dalam 9.2. Kebijakan eksternal ditujukan untuk pelapor, pengguna, dan pemangku kepentingan lainnya. Vendor juga dapat membuat kebijakan internal yang sesuai. Kebijakan internal ditujukan bagi karyawan atau agen yang melakukan pengungkapan kerentanan untuk vendor. Kedua kebijakan tersebut sebaiknya sejalan.

Kebijakan internal dapat berisi rincian lebih lanjut, informasi pribadi, dan proses yang diperlukan untuk alasan internal dan untuk memenuhi kebijakan eksternal.

Setiap vendor memiliki persyaratan dan sumber daya berbeda yang tersedia untuk menangani informasi kerentanan keamanan. Vendor sebaiknya mengembangkan kebijakan sebelum terlibat dalam pengungkapan kerentanan. Mengembangkan kebijakan merupakan bagian dari fase Persiapan yang dideskripsikan pada 5.6.2. Kebijakan pengungkapan sebaiknya menyatakan intensi vendor, tanggung jawabnya serta apa yang diharapkan vendor dari pemangku kepentingan lainnya. Kebijakan pengungkapan kerentanan sebaiknya sederhana dan jelas untuk memfasilitasi pelaporan kerentanan yang mudah kepada vendor. Vendor sebaiknya mempertimbangkan penempatan intuitif kebijakan pengungkapan mereka dan informasi relevan lainnya. Salah satu lokasi tersebut dapat berupa halaman web keamanan (misalnya, www.example.com/security).

9.2 Elemen kebijakan yang disyaratkan

9.2.1 Umum

Kebijakan pengungkapan kerentanan harus mencakup elemen berikut.

9.2.2 Preferensi mekanisme kontak

Provisi pada 6.2.1 mensyaratkan vendor untuk menyediakan satu atau beberapa mekanisme yang secara teknis terkini dan dapat digunakan untuk menerima laporan. Vendor harus menyertakan informasi tentang mekanisme kontak ini dalam kebijakan pengungkapan kerentanan vendor.

Mekanisme kontak dapat termasuk satu atau beberapa hal berikut:

a) alamat surel. Contoh alias surel yang dapat digunakan antara lain sebagai berikut:

   — security-alert@example.com;

   — security@example.com;

   — secure@example.com;

   — psirt@example.com;

   — csirt@example.com;

b) nomor telepon;

c) formulir web. Keuntungan mekanisme ini termasuk kemampuan yang lebih besar untuk mempengaruhi isi laporan (misalnya, vendor dapat membedakan antara informasi opsional dan wajib) dan integrasi yang lebih baik dengan basis data laporan kerentanan;

d) informasi kontak untuk layanan pelanggan, jika layanan pelanggan dilatih untuk menerima laporan kerentanan.

9.3 Elemen kebijakan yang direkomendasikan

9.3.1 Umum

Kebijakan pengungkapan kerentanan sebaiknya termasuk elemen berikut.

9.3.2 Isi laporan kerentanan

Vendor dapat berharap untuk memperoleh informasi yang mungkin berguna untuk memahami kerentanan dan kemungkinan remediasi dan mitigasi. Vendor dapat menyediakan formulir untuk tujuan ini (lihat 6.2.1).

Dalam kasus ketika kerentanan berdampak pada multipel vendor, akan berguna bagi vendor untuk mengetahui apakah pelapor juga telah melaporkan kerentanan kepada vendor lainnya yang terdampak.

9.3.3 Pilihan komunikasi yang aman

Vendor sebaiknya menyediakan kanal komunikasi yang aman menggunakan teknologi TLS, S/MIME, atau OpenPGP. Jika vendor menyediakan mekanisme pelaporan berbasis web, mekanisme tersebut harus menggunakan TLS (HTTPS) atau sistem kriptografi serupa yang banyak digunakan, yang melindungi konfidensialitas pengiriman dan mengautentikasi situs web. Vendor sebaiknya mengonfigurasi kapabilitas tersebut sebelum berkomunikasi dengan pelapor.

9.3.4 Penetapan ekspektasi komunikasi

Vendor sebaiknya mengeset ekspektasi untuk komunikasi, termasuk pengakuan awal dan pembaruan status. Vendor sebaiknya menyediakan informasi terkini kepada pelapor dengan menggunakan metode komunikasi yang telah disetujui.

Penting bagi vendor untuk menjaga dialog yang terbuka dan kooperatif dengan pelapor sehingga informasi kerentanan dapat dibagikan dan risiko terhadap pengguna dapat dikurangi seefisien mungkin. Jika vendor menentukan bahwa pelapor tidak menyediakan informasi yang cukup, vendor dapat menghubungi pelapor untuk meminta detail
tambahan. Vendor bertindak sebagai pelapor atau koordinator berkomunikasi dengan vendor lain dalam rantai pasokannya. Kebijakan sebaiknya mendukung semua kemungkinan komunikasi tersebut.

Pada sebagian besar kasus, tim yang berurusan dengan laporan kerentanan tidak dapat berurusan dengan insiden keamanan dan pertanyaan terkait keamanan lainnya. Kebijakan ini dapat menentukan titik kontak untuk tipe permintaan lainnya tersebut.

Kebijakan ini dapat mendeskripsikan mekanisme yang digunakan untuk melacak laporan dan komunikasi dengan pelapor dan pemangku kepentingan lainnya.

9.3.5 Ruang lingkup

Vendor sebaiknya mendeskripsikan produk dan layanan yang memenuhi syarat untuk menerima remediasi. Vendor sebaiknya juga mendeskripsikan produk dan layanan yang tidak memenuhi syarat untuk menerima remediasi. Misalnya, suatu produk dapat berada dalam fase pengujian atau tidak lagi didukung.

9.3.6 Publikasi

Vendor sebaiknya mendeskripsikan bagaimana advisori dan remediasi didistribusikan.

9.3.7 Pengakuan

Vendor sebaiknya mendeskripsikan bagaimana pelapor diakui atas upayanya. Pengakuan dapat termasuk penghargaan dalam advisori, hadiah, dan uang hadiah.

9.4 Elemen kebijakan opsional

9.4.1 Umum

Kebijakan pengungkapan kerentanan dapat berisi elemen berikut.

9.4.2 Pertimbangan hukum

Tindakan menemukan atau melaporkan kerentanan dapat melanggar hukum atau regulasi lainnya. Vendor dapat mempertimbangkan untuk tidak mengambil tindakan hukum terhadap pelapor yang secara sukarela, dengan itikad baik, melaporkan kerentanan.

9.4.3 Lini masa pengungkapan

Vendor dapat memublikasikan lini masa yang diharapkan untuk respons dan pengungkapan.

Lampiran A
(informatif)
Contoh pengungkapan kebijakan kerentanan

A.1 Facebook

https://www.facebook.com/whitehat

A.2 CERT/CC

https://www.cert.org/vulnerability-analysis/vul-disclosure.cfm [1)]

A.3 Zero Day Initiative

http://www.zerodayinitiative.com/advisories/disclosure_policy/ [1)]

A.4 Cisco

http://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html [1)]

A.5 NCSC-FI

https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices/vulnerabilitycoordination.html [1)]

https://www.viestintavirasto.fi/attachments/vulncoord/68RKIxXES/Vulncoord_policy_1.1.pdf [1)]

A.6 NCSC-NL

https://www.ncsc.nl/english/security [1)]

https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html [1)]

https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/news/responsible-disclosure-guideline/1/Responsible%2BDisclosure%2BENG.pdf [1)]

A.7 Rapid7

https://www.rapid7.com/disclosure/ [1)]

---

[1] Diambil pada 2017-05-18.

Lampiran B
(informatif)
Informasi yang diminta dalam suatu laporan

Informasi yang diminta dari pelapor bervariasi berdasarkan pilihan spesifik vendor dan produk atau layanan yang terdampak.

Informasi berikut ini dapat berguna ketika menyampaikan laporan kepada vendor:

a) informasi nama produk atau layanan, URL, atau versi yang terdampak;

b) sistem operasi dari komponen yang terlibat;

c) informasi versi;

d) deskripsi teknis terkait tindakan yang dilakukan dan hasilnya dengan sedetail mungkin;

e) sampel kode yang pernah digunakan untuk mengetes atau mendemonstrasikan kerentanan;

f) informasi kontak pelapor;

g) pihak lain yang terlibat;

h) rencana pengungkapan;

i) detail asesmen ancaman/risiko dari ancaman dan/atau risiko yang teridentifikasi termasuk level risiko (tinggi, sedang, rendah) untuk hasil asesmen;

j) konfigurasi perangkat lunak dari komputer atau konfigurasi perangkat pada saat menemukan kerentanan;

k) informasi yang relevan tentang komponen dan perangkat yang terhubung jika kerentanan muncul selama interaksi. Ketika komponen atau perangkat sekunder memicu kerentanan, detail tersebut harus disediakan;

l) waktu dan tanggal diskoveri;

m) informasi peramban termasuk informasi tipe dan versi.

Lampiran C
(informatif)
Contoh advisori

C.1 Contoh advisori

Contoh berikut mendeskripsikan kerentanan fiktif yang berdampak pada produk dan vendor fiktif.

ROB-2017-004: Prosesor Robotron R.U.R. rentan terhadap serangga terbang

Tanggal

2016-11-25

Ringkasan

Sebuah kerentanan telah ditemukan di prosesor R.U.R. model 48, 49 dan 51 pada *mainframe* Robotron. Kerentanan ini dapat digunakan untuk mengelevasi privilese eksekusi proses.

Kerentanan ini diberi ID CVE yaitu CVE-2016-000111. ID untuk Bug internal adalah RT12345.

Teks lengkap advisori ini dapat ditemukan di https://www.robotron.example.com/advisories/ROB-2017-004.html>. Seluruh advisori dipublikasikan oleh Robotron Corporation dan *hash* SHA-512 mereka tersedia di <https://www.robotron.example.com/advisories/>. *Hash* SHA-512 untuk advisori ini adalah ABCDEF123456567890.

Produk yang terdampak

Model *mainframe* Robotron berikut ini terdampak kerentanan ini:

Model 1;
Model 2;
Model 2a;
Model 4.

Model *mainframe* Robotron berikut tidak terdampak kerentanan ini:

Model 3;
Model 5.

Tidak ada produk Robotron lain yang terdampak kerentanan ini.

Bagaimana memverifikasi apakah produk terdampak

Untuk memverifikasi apakah *mainframe* Anda terdampak kerentanan ini mohon melakukan langkah-langkah berikut.

Matikan sistem operasi.
Putuskan sambungan daya dari rak CPU.
Buka panel belakang rak CPU.
Temukan papan prosesor. Secara bawaan, ini terletak di slot pertama dari kiri. Papan prosesor ditandai dengan kata “CPU” di bagian ujung.
Cabut papan dan periksa sudut kanan atas. Ini harus berisi informasi model dan revisi HW prosesor.

Mainframe anda terdampak kerentanan ini jika model prosesornya adalah “R.U.R.” dan revisi HW adalah salah satu dari berikut ini: 48, 49 atau 51.

Deskripsi kerentanan

Kerentanan ini dapat dipicu oleh serangga terbang yang panjangnya sekitar 7 mm. Serangga tersebut dapat secara elektrik menghubungkan kawat pada papan prosesor. Kawat yang terhubung akan mengindikasikan kepada prosesor bahwa proses yang saat ini sedang dieksekusi harus diberikan privilese pengguna super.

Hal ini tidak dapat dilakukan oleh serangga yang tidak dapat terbang karena kabel daya yang terkspos di bagian tepi papan prosesor akan mencegah serangga untuk mencapai area yang dimaksud (diposisikan ke arah tengah papan).

Dampak

Dengan mengeksploitasi kerentanan ini, adalah mungkin untuk mengelevasi hak istimewa sebuah proses yang saat ini sedang dieksekusi. Setelah mengelevasi hak istimewa, proses tersebut dapat mengeksekusi perintah sebagai pengguna super dan memodifikasi setiap aspek dari *mainframe*.

Tingkat keparahan

Skor CVSSv3 untuk kerentanan ini adalah: 6.4 (Basis) and 5.8 (Temporal)

CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Remediasi

Solusi sementara (*workaround*) untuk kerentanan ini adalah tidak membiarkan serangga terbang ke dalam ruang *mainframe* (yaitu dengan menjaga jendela dan pintu tetap tertutup).

Untuk meremediasi kerentanan ini, pengguna mengunduh perangkat tegar (*firmware*) dari laman web pendukung R.U.R. pada URL. Instruksi bagaimana cara menginstal perangkat tegar (*firmware*) disertakan di laman web yang sama.

Setelah mengunduh perangkat tegar (*firmware*) pengguna memverifikasi bahwa *hash* SHA-512 cocok dengan yang dipublikasikan pada laman pendukung.

Jangan menginstal perangkat tegar (*firmware*) yang *hash*-nya tidak cocok dengan yang dipublikasikan. Jika demikian segera beri tahu Layanan Pendukung Robotron tentang masalah tersebut.

Kredit

Kerentanan ini ditemukan secara independen oleh Grace Hooper dan Ada Lovelace.

Informasi kontak

Pelanggan dan pengguna peralatan Robotron sebaiknya melaporkan semua potensi kerentanan keamanan ke psirt@robotron.example.com. Semua laporan akan diakui dalam waktu 48 jam.

Untuk masalah nonkeamanan pelanggan harus mengontak Layanan Pendukung Robotron melalui surel di service@robotron.example.com atau menelepon nomor telepon yang terdaftar di <https://www.robotron.example.com/contact.html>.

Riwayat revisi

Versi	Tanggal	Komentar
1.0	2016-11-04	Publikasi awal
1.1	2016-11-11	Revisi HW 51 diidentifikasi sebagai kerentanan. Versi sebelumnya advisori ini tersedia di <URL-rev1.0>

Syarat penggunaan

Advisori ini dapat didistribusikan secara bebas seluruhnya atau sebagian dengan syarat URL advisori disertakan. URL harus tidak mengarah ke situs selain Robotron. Robotron Corporation tidak […]

C.2 *Heap memory corruption in ASN.1 parsing code generated by Objective Systems Inc. ASN1C compiler for C/C++*

https://github.com/programa-stic/security-advisories/tree/master/ObjSys/CVE-2016-5080 [2)]

C.3 *Multiple Vulnerabilities in Network Time Protocol Daemon Affecting Cisco Products: November 2016*

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161123-ntpd [2)]

C.4 *RHSA-2017:0057 — Security Advisory*

https://access.redhat.com/errata/RHSA-2017:0057 [2)]

C.5 *Alert (TA10-159A) Adobe Flash, Reader, and Acrobat Vulnerability*

https://www.us-cert.gov/ncas/alerts/TA10-159A [2)]

---

[2] Retrieved on 2017-05-18.

Lampiran D
(informatif)
Ringkasan unsur normatif

Subpasal	Elemen normatif
5.3.1 ISO/IEC 30111	ISO/IEC 30111 harus digunakan secara bersamaan dengan dokumen ini.
6.2.2 Kapabilitas untuk menerima laporan	Vendor harus menyediakan satu atau lebih mekanisme yang secara teknis terkini dan dapat digunakan untuk menerima laporan potensi kerentanan.
6.2.3 Monitoring	Vendor harus memonitor mekanisme pelaporan mereka untuk laporan dan komunikasi baru yang berkaitan dengan laporan yang sudah ada.
6.2.5 Pengakuan laporan	Vendor harus mengakui penerimaan laporan potensi kerentanan dalam 7 hari kalender.
6.3 Asesmen awal	Vendor harus melakukan asesmen awal, atau triase, terhadap laporan kerentanan. Jika vendor tidak menganggap laporan sebagai kerentanan, vendor harus menginformasikan pelapor dan pemangku kepentingan lainnya.
6.4 Investigasi lebih lanjut	Untuk laporan yang mensyaratkan investigasi lebih lanjut atau dianggap sebagai kerentanan yang valid, vendor harus memulai proses penanganan kerentanan.
6.5 Komunikasi yang sedang berlangsung	Selama penanganan kerentanan, vendor harus berkomunikasi dengan pelapor dan pemangku kepentingan lainnya.
7.4.2 Pengidentifikasi	Advisori harus berisi pengidentifikasi tertentu. Pengidentifikasi advisori: Suatu advisori harus dilabeli dengan pengidentifikasi yang unik dan konsisten untuk dokumen advisori tersebut; Pengidentifikasi kerentanan: Suatu advisori harus menyediakan pengidentifikasi yang unik dan konsisten untuk kerentanan yang dituju dalam advisori.
4.3 Tanggal dan waktu	Advisori harus mengindikasikan tanggal publikasi awal dan mungkin menyertakan tanggal lainnya, misalnya, sebagai bagian dari riwayat revisi. Advisori harus menggunakan referensi tanggal dan waktu yang tidak ambigu dan menggunakan ISO 8601.
7.4.6 Produk terdampak	Advisori harus menyediakan informasi yang cukup bagi pengguna untuk menentukan apakah mereka terdampak oleh kerentanan atau tidak.
7.7 Autentisitas advisori	Vendor harus menyediakan kemampuan untuk mengautentikasi dan memverifikasi integritas advisori.

Subpasal	Elemen normatif
7.8.2 Autentisitas remediasi	Jika pengguna disyaratkan mengambil tindakan untuk mengaplikasikan remediasi, maka vendor harus menyediakan kemampuan untuk mengautentikasi dan memverifikasi integritas remediasi.
9.1 Umum	Untuk menyampaikan intensi dan ekspektasi, vendor harus mengembangkan dan memublikasikan kebijakan pengungkapan kerentanan eksternal. Kebijakan harus memuat unsur yang disyaratkan dalam 9.2.
9.2.1 Umum	Kebijakan pengungkapan kerentanan harus mencakup elemen berikut.
9.2.2 Preferensi mekanisme kontak	Vendor harus menyertakan informasi tentang mekanisme kontak ini dalam kebijakan pengungkapan kerentanan vendor.
9.3.3 Pilihan komunikasi yang aman	Jika vendor menyediakan mekanisme pelaporan berbasis web, mekanisme tersebut harus menggunakan TLS (HTTPS) atau sistem kriptografi serupa yang banyak digunakan, yang melindungi konfidensialitas penyampaian dan mengautentikasi situs web.

Bibliografi

[1] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

[2] ISO/IEC 27010, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*

[3] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on* ISO/IEC 27002 *for cloud services*

[4] ISO/IEC 27034-1, *Information technology — Security techniques — Application security — Part 1: Overview and concepts*

[5] ISO/IEC 27034-5, *Information technology — Security techniques — Application security — Part 5: Protocols and application security controls data structure*

[6] ISO/IEC 27035-1, *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*

[7] ISO/IEC 27036-3, *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security*

[8] ISO 8601, *Data elements and interchange formats — Information interchange — Representation of dates and times*

[9] ITU-T X.1520, *Common vulnerabilities and exposures*

[10] ITU-T X.1521, *Common vulnerability scoring sistem*

[11] ITU-T X.1524, *Common weakness enumeration*

[12] COMMON V.R.F. (CVRF). *Industry Consortium for Advancement of Security on the Internet* (ICASI). *Available at* <https://www.icasi.org/the-common-vulnerability-reporting-framework-cvrf-v1-1/>

[13] COMMON V.R.F. (CVRF). OASIS *Common Security Advisory Framework* (CSAF) TC. *Available at* <https://www.oasis-open.org/committees/csaf/charter.pdf>

[14] *Vulnerability Disclosure Attitudes and Actions*. NTIA *Multistakeholder Process: Cybersecurity Vulnerabilities. Available at* <https://www.ntia.doc.gov/files/ntia/publikations/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf>

[15] ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security*

[16] ISO/IEC 18405, *Information technology — Security techniques — Methodology for IT security evaluation*

Information technology — Security techniques — Vulnerability disclosure

1 Scope

This document provides requirements and recommendations to vendors on the disclosure of vulnerabilities in products and services. Vulnerability disclosure enables users to perform technical vulnerability management as specified in ISO/IEC 27002:2013, 12.6.1[1]. Vulnerability disclosure helps users protect their systems and data, prioritize defensive investments, and better assess risk. The goal of vulnerability disclosure is to reduce the risk associated with exploiting vulnerabilities. Coordinated vulnerability disclosure is especially important when multiple vendors are affected. This document provides:

— guidelines on receiving reports about potential vulnerabilities;

— guidelines on disclosing vulnerability remediation information;

— terms and definitions that are specific to vulnerability disclosure;

— an overview of vulnerability disclosure concepts;

— techniques and policy considerations for vulnerability disclosure;

— examples of techniques, policies (Annex A), and communications (Annex B).

Other related activities that take place between receiving and disclosing vulnerability reports are described in ISO/IEC 30111.

This document is applicable to vendors who choose to practice vulnerability disclosure to reduce risk to users of vendors' products and services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
vulnerability
functional behaviour of a product or service that violates an implicit or explicit security policy

Note 1 to entry: ISO/IEC 27002:2013, 12.6.1[1] uses the term “technical vulnerability” to distinguish between the more general risk-based concept of vulnerability and the term used in this document.

3.2
disclosure
act of initially providing *vulnerability* (3.1) information to a party that was not believed to be previously aware

3.3
coordination
set of activities including identifying and engaging stakeholders, mediating, communicating, and other planning in support of *vulnerability* (3.1) *disclosure* (3.2)

Note 1 to entry: The term “coordinated vulnerability disclosure” is used to denote a disclosure process that includes coordination.

3.4
vendor
individual or organization that is responsible for remediating vulnerabilities

Note 1 to entry: A vendor can be the developer, maintainer, producer, manufacturer, supplier, installer, or provider of a product or service.

3.5
reporter
individual or organization that notifies a *vendor* (3.4) or *coordinator* (3.6) of a potential *vulnerability* (3.1)

Note 1 to entry: There are no special requirements for acting as a reporter. Reporters can be individuals, organizations, amateurs or hobbyists, professionals, end-users, security research organizations, vendors, governments, or coordinators.

Note 2 to entry: The term “reporter” does not imply unique or original discovery or reporting.

Note 3 to entry: Reporters can be called researchers, whether or not the reporter explicitly performs security or vulnerability research. Historically, this role is also referred to as “finder.”

3.6
coordinator
individual or organization that performs *coordination* (3.3)

3.7
remediation
change made to a product or service to remove or mitigate a *vulnerability* (3.1)

Note 1 to entry: A remediation typically takes the form of a binary file replacement, configuration change, or source code patch and recompile. Different terms used for

“remediation” include patch, fix, update, hotfix, and upgrade. Mitigations are also called workarounds or countermeasures.

3.8
advisory
document or message that provides *vulnerability* (3.1) information intended to reduce risk

Note 1 to entry: An advisory is meant to inform users or other stakeholders about a vulnerability including, if possible, how to identify and remediate vulnerable systems.

4 Abbreviated terms

COTS	common off-the-shelf
CRM	customer relationship management
CSIRT	computer security incident response team
CVE	common vulnerabilities and exposures[9]
CVRF	common vulnerability reporting format[12][13]
CVSS	common vulnerability scoring system[10]
CWE	common weakness enumeration[11]
HTTP(S)	hypertext transfer protocol (secure)
ICT	information and communication technology
OpenPGP	open pretty good privacy
OWASP	open web application security project
PoC	proof of concept
PSIRT	product security incident response team
S/MIME	secure multipurpose internet mail extensions
SQL	structured query language
TLS	transport layer security

5 Concepts

5.1 General

The purpose of this clause is to provide background information and context to help understand vulnerability disclosure.

Vulnerability disclosure involves different stakeholders with different perspectives, incentives, capabilities, and available information. Furthermore, communication and process synchronization among multiple stakeholders can quickly become complicated. In practice, disclosure can deviate from the activities described in this document due to a variety of unforeseen circumstances.

5.2 Structure of this document

This document is meant to be read in its entirety as input to the development or improvement of vulnerability disclosure policies and processes. The remaining clauses of this document are organized as follows:

— Clause 5: Concepts;

— Clause 6: Receiving vulnerability reports;

— Clause 7: Publishing vulnerability advisories;

— Clause 8: Coordination;

— Clause 9: Vulnerability disclosure policy.

The structure of this document is not meant to be followed in strict sequence as it appears above. For example, a vendor should ideally develop policy (Clause 9) before starting to receive reports (Clause 6).

Annex D contains a summary of all of the normative elements in this document.

5.3 Relationships to other International Standards

5.3.1 ISO/IEC 30111

ISO/IEC 30111 shall be used in conjunction with this document. The relationship between the two International Standards is illustrated in Figure 1.

This document provides guidelines for vendors to include in their normal business processes when receiving reports about potential vulnerabilities from external individuals or organizations and when distributing vulnerability remediation information to affected users.

ISO/IEC 30111 gives guidelines on how to investigate, process, and resolve potential vulnerability reports.

While this document deals with the interface between vendors and reporters, ISO/IEC 30111 deals with internal vendor processes including the triage, investigation, and remediation of vulnerabilities, whether the source of the report is external to the vendor or from within the vendor’s own security, development, or testing teams.

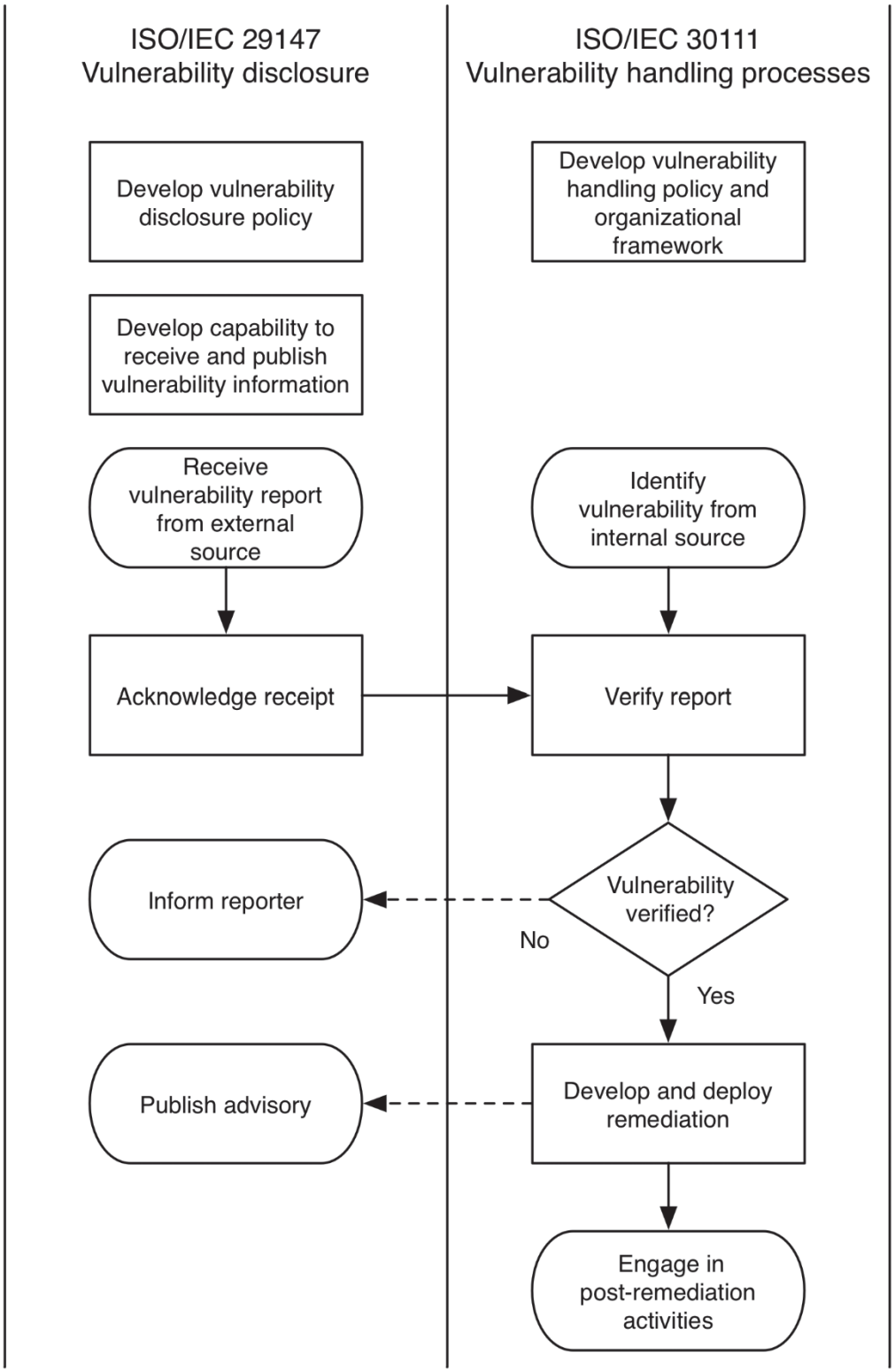


Figure 1 — Relationship between ISO/IEC 29147 and ISO/IEC 30111

5.3.2 ISO/IEC 27002

Vulnerability disclosure enables the management of technical vulnerabilities (ISO/IEC 27002:2013, 12.6.1[1]).

5.3.3 ISO/IEC 27034 series

Application security seeks to reduce the creation of application vulnerabilities (see ISO/IEC 27034-1:2011, 6.5.2[4]). Vulnerability disclosure can demonstrate the need for changes to application security practices. Vulnerability disclosure cannot demonstrate that application security is completely effective.

Vulnerability disclosure occurs in the utilization and maintenance phases of the application security lifecycle reference model described in ISO/IEC TS 27034-5-1:2018, 6.3.13 and 6.3.14[5].

5.3.4 ISO/IEC 27036-3

Vulnerability disclosure supports multiple aspects of ICT supply chain security described in ISO/IEC 27036-3:2013, 5.4 a), 5.8 i), 6.1.1 a) 2) and 6.3.4 [7].

5.3.5 ISO/IEC 27017

Vulnerability disclosure is necessary to enable the management of technical vulnerabilities as specified for cloud services in ISO/IEC 27017:2015, 12.6.1[3].

5.3.6 ISO/IEC 27035 series

Some incident management plans, particularly those of vendors, include vulnerability disclosure (see ISO/IEC 27035-1:2016, Introduction[6]). Such plans typically treat vulnerability disclosure as a type of incident. Incident management can also include vulnerability management (see also ISO/IEC 27002:2013, 12.6.1[1]), which is only possible when vulnerabilities are disclosed.

5.3.7 Security evaluation, testing and specification

This document provides guidance for vulnerability reports received externally, and not through organized internal assurance and evaluation efforts. Thus, the more formal testing, assurance, and evaluation standards ISO/IEC 15408[15] and ISO/IEC 18405[16] do not generally apply.

5.4 Systems, components, and services

5.4.1 Systems

A system is a set of connected components and services. In vulnerability disclosure, the causes of a vulnerability can be unclear, or due to interactions between the parts of a system, or between systems. Thus, it is sometimes necessary to talk about systems being affected by vulnerabilities.

5.4.2 Components

A component is a unit of software or hardware that can be both an entire system unto itself and used as part of a larger system. A component can be an entire operating system, a chip, an application, a package, a library, or even a single file or segment of source code.

For the purposes of this document, the distinction between hardware and software components is seldom relevant. There are very few cases of vulnerabilities in pure hardware components. In most cases, so-called “hardware” vulnerabilities actually occur in low-level software or firmware.

5.4.3 Products

A product is usually one or more components or a system. Products are provided by vendors to users either for sale or for free, usually under licensing terms. There are many different types of products including but not limited to, custom software built under contract for a specific user's licenced use, libraries intended to be included in other products, commercial off-the-shelf (COTS) products for mass markets, community-developed projects, and recreational or hobbyist offerings.

5.4.4 Services

A service is a collection of features provided to users. Users can interact with services they do not own, operate, or maintain.

For vulnerability disclosure, vulnerabilities in services maintained by the vendor can usually be remediated by the vendor taking action. Users can have to take action as well in order to remediate the vulnerability. For example, a vendor implements changes on their own infrastructure to remediate the vulnerability, and users have to change their passwords after the vendor has implemented the changes.

5.4.5 Vulnerability

A vulnerability is generally a behaviour or set of conditions that allows the violation of an explicit or implicit security policy. Typically, the violation of a user's security policy results in a negative impact or loss to the user. One common way to categorize loss is to consider the impact to the confidentiality, integrity, and availability of an asset. For example, a vulnerability that allowed an attacker to install malicious software on a user's system impacts confidentiality and integrity since the attacker can use the malicious software to read or change sensitive information. A vulnerability in a network product that caused the product to experience a system error would impact availability. The actual impact of a vulnerability depends on how the vulnerable product is used and other contextual factors.

Vulnerabilities are often caused by implementation defects in software. A vulnerability can be associated to the security policy if one exists. One common type of vulnerability includes buffer overflows and related low-level memory management errors that allow specially crafted input to control execution of the vulnerable software program. SQL injection and cross-site scripting vulnerabilities are common types of vulnerabilities found in web applications. Many other sets of conditions can cause or contribute to vulnerabilities, including design decisions, default configuration settings, weak authentication or access control, lack of awareness or education, or even unexpected interactions between systems or changes in operating environments.

More information about types of vulnerabilities can be found in CWE and OWASP. Both of these resources help developers and engineers to recognize and avoid creating security vulnerabilities.

Many stakeholders (predominantly vendors and users) seek to identify and resolve vulnerabilities, either removing them entirely (usually by patching or updating software to remove defects) or by mitigating or working around vulnerabilities to reduce the likelihood or impact of successful attack. Vulnerability disclosure provides vendors and users with information to resolve and mitigate vulnerabilities and to make better risk decisions.

Attackers also seek to identify vulnerabilities, but typically do not attempt to disclose or resolve vulnerabilities. Attackers seek to exploit vulnerabilities for some gain, almost always causing loss to users.

5.4.6 Product interdependency

Many products are complex systems that include or are dependent upon other products or components in some way. It is possible that a user or vendor is not initially be certain which products are affected by the vulnerability. These interdependencies are important since products that use or interact with a vulnerable product can also be vulnerable.

Product dependencies can include:

— source code re-use from other products, software libraries, or other types of interfaces;

— hardware or software supply chain;

— rebranding by different vendors of the same core technology;

— use of the same protocols or formats.

Depending on sales, distribution, and support models, vendors can have accurate lists of users or not. This can be relevant when considering notifying affected users of a vulnerability.

5.5 Stakeholder roles

5.5.1 General

This subclause describes significant stakeholder roles in vulnerability disclosure. Stakeholders are individuals, groups, or organizations that act in one or more roles.

5.5.2 User

Users can directly operate software or hardware products or make use of a service. Users can be referred to as consumers, customers, or end-users. Due to the interdependencies of modern software products, users might not know precisely which products or services they are actually using.

Users need information about vulnerabilities, particularly remediation, in order to make effective risk decisions and to use software products and services more securely. Publishing vulnerability information is discussed in Clause 7.

5.5.3 Vendor

There are a number of different terms used to describe individuals or organizations who create or provide software products, including manufacturer, developer, maintainer, or distributor. Similarly, an individual or organization that delivers software products within a supply chain can be called a supplier. For the purposes of this document, the term “vendor” is used to mean all of these individuals and organizations. A vendor can be an individual, a small team, a large commercial enterprise, or an open source project.

Vendors are responsible for the security of their products and services. Vendors carry out vulnerability disclosure to receive reports about vulnerabilities, develop remediations, and publish advisories.

There are many types of vendors with various models for developing, selling, supporting, and distributing products. Some vendors integrate products into a system or service, and these vendors may act as customers or users of the component products. Such vendors can be dependent on component vendors for vulnerability remediation information.

5.5.4 Reporter

The reporter notifies a vendor of a potential vulnerability. A reporter usually, but not always, finds or discovers the vulnerability. The discovery may not be the first or only discovery. For the purposes of this document, it is assumed that a reporter will attempt to inform a vendor or coordinator about a vulnerability. In practice, a reporter can choose not to attempt to inform a vendor or coordinator, or the attempt can fail. Receiving vulnerability reports is discussed in Clause 6.

A reporter is often a security researcher, but it is important to reinforce that any individual or organization can act as a reporter. Professional researchers can operate independently or as part of an organization. Some researchers are associated with universities or other academic institutions. Other reporters do not regularly perform security analysis or research but identify vulnerabilities in the course of other activity or even by accident. Vendors, users, and coordinators can all act as reporters.

The variety of reporters has implications for the quality of vulnerability reports and the familiarity of the reporter with disclosure practices.

Reporters are sometimes concerned with legal or other pressure brought to bear on them. Such pressure can have a “chilling effect,” decreasing the likelihood of reporting.

5.5.5 Coordinator

A coordinator generally acts as intermediaries between a reporter and vendor. Common services provided by a coordinator include:

— identifying and contacting vendors;

— managing vulnerabilities that affect multiple vendors;

— performing technical analysis and validation;

— negotiating disclosure timelines;

— supporting reporters;

— publishing advisories;

— educating vendors and reporters about the disclosure process.

It is not necessary for coordinators to be involved in every disclosure. For cases involving one or a small number of vulnerabilities affecting a single vendor, a reporter and vendor are often sufficient. Coordinators can aid negotiations when multiple vendors are affected, reporters and vendors disagree, or other complexities arise.

Coordinators may work with other coordinators to obtain help with domain expertise, language, geographic, and cultural barriers and to share resources and effort. Some computer security incident response teams (CSIRTs) provide broad vulnerability coordination services on an operational basis, while other CSIRTs coordinate in more limited ways, for example, covering specific regions, industries, or on an as-needed basis.

Some vendors and governments provide free coordination services while some vendors offer commercial coordination services.

Some vendors provide coordination services, as do some commercial security vendors. For example, some organizations pay reporters for vulnerability reports, use the vulnerability information to provide commercial protection to their customers, and also act as coordinators, disclosing privately to vendors and later to the public. There are variations and degrees of commercially-oriented vulnerability coordination offerings.

While coordinators often have interests in protecting their constituencies, coordinators should attempt to be technically objective and minimize risk to all stakeholders.

Coordination is further described in Clause 8.

5.6 Vulnerability handling process summary

5.6.1 General

This subclause summarizes the vulnerability handling process that is described further in ISO/IEC 30111. Figure 2 outlines the vendor's vulnerability handling process including a preliminary step to develop a vulnerability disclosure policy and capabilities.

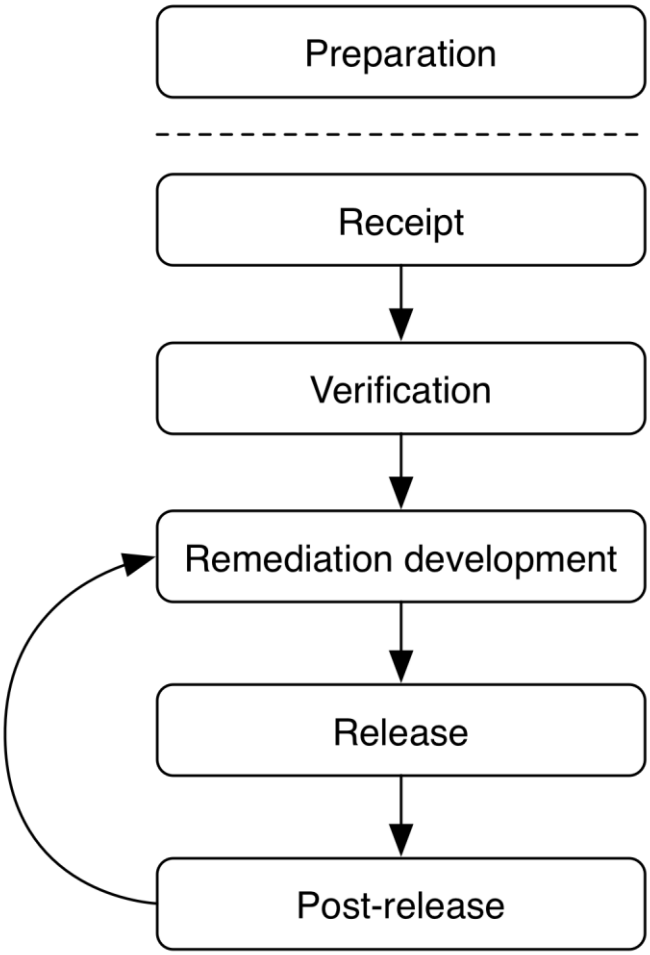


Figure 2 — Summary vulnerability handling process

5.6.2 Preparation

Vendors should develop policy (see Clause 9), processes, and capability before starting a vulnerability disclosure program. Preparation can involve creating a response organization (often called a PSIRT or CSIRT), hiring and assigning staff, developing tools, and publishing information about the program.

Vendors should consider performing vulnerability assessments of products and services in scope of the program. Such assessments can identify easily discovered vulnerabilities and reduce the number of reports before the program starts.

5.6.3 Receipt

A reporter identifies potential vulnerabilities in products or services and notifies the vendor. The vendor acknowledges receipt of the report.
If a vendor is not able to receive a vulnerability report, the reporter or coordinator may decide to publish an advisory without the vendor's prior knowledge. A reporter, or anyone in possession of vulnerability information can disclose or publish the information at any time.

Receiving vulnerability reports is described in Clause 6.

5.6.4 Verification

The vendor investigates the report. Investigation often involves attempting to reproduce the environment and behaviour reported by the reporter. This can be a preliminary investigation, focused primarily on the need for further effort by the vendor. Investigation can also include correlating similar or related reports, assessing severity, and determining other affected products. The investigation determines whether the report constitutes a vulnerability or not. The vendor may communicate with the reporter during the investigation, and the vendor notifies the reporter of the results at the end of the investigation. This phase is often called "triage."

5.6.5 Remediation development

The vendor develops remediations for vulnerabilities. Remediation development can involve more detailed investigation of the root cause of the vulnerabilities and determination of other products affected by the same or similar vulnerabilities. The vendor typically develops remediation and mitigation techniques and performs positive tests to determine that the remediation works correctly, and negative (regression) tests to provide assurance that the remediation does not disrupt existing functionality.

The vendor should feed the information about the vulnerability and root cause analysis back into the software development lifecycle or deployment guidelines, in order to avoid introducing the same type of vulnerability in the future. See also ISO/IEC 27034-1[4].

5.6.6 Release

The vendor develops and securely distributes the remediation. For a product, the vendor provides the remediation and mitigation information to users, typically in the form of a vulnerability advisory and software patches or updates, and users deploy the remediation.

For a service vulnerability, the vendor deploys remediation and optionally discloses the vulnerability.

A vendor may release an advisory before a remediation is available, particularly in cases of active exploitation or public discussion. The vendor should attempt to ensure the remediation does not introduce new vulnerabilities, overall product quality issues, or have compatibility problems with other products or services if possible.

An important reason for informing users about a vulnerability is that users often need to take action to remediate and re-assess their risk. When remediating a vulnerability in a service, it is possible that there is no need for users to take any action. There are, however, other reasons to publish vulnerability information, including:

— support for incident or forensic investigations, knowing when a vulnerability existed (and was not remediated);

— improved secure design, engineering, and development practices;

— transparency and accountability, informing users and other stakeholders that vulnerabilities are identified and remediated;

— assurance, informing users of non-vulnerability;

— providing authoritative information, disambiguation, clarification;

— informing public policy decisions;

— documenting system changes for development and operational use;

— providing acknowledgment and credit to reporters.

Considering reasons beyond the need for user action, a service can still choose to publish vulnerability information.

Publishing vulnerability advisories is described in Clause 7.

5.6.7 Post-release

A vendor collects feedback from users and updates remediation and mitigation information as necessary. For example, a remediation can be found to be incomplete or to cause regression issues or side effects.

5.6.8 Embargo period

In order to give vendors time to develop remediations without attackers also having access to public vulnerability information, reporters often notify vendors privately and do not disclose publicly until remedations are ready or an embargo period has elapsed. The receipt, verification, and remediation development phases are typically covered by the embargo period.

Reporters and other with knowledge of a vulnerability have the ability to disclose publicly at any time. Reporters use different embargo periods, which are sometimes negotiable.

5.7 Information exchange during vulnerability disclosure

Figure 3 illustrates information exchange during vulnerability disclosure. There are two main exchanges: Potential vulnerability reports from reporters to vendors, and advisories from vendors to users. A potential vulnerability report is sent from a reporter to a vendor either directly or through a coordinator. A vendor may act as a reporter and report a vulnerability to

another vendor. An advisory is released by a vendor either privately to its users or, more commonly, to the public. This document focuses on these two exchanges from the perspective of the vendor receiving vulnerability reports and publishing remediation information.

A complete vulnerability disclosure process can include multiple disclosure events, such as a reporter reporting to a vendor, a vendor publishing an advisory, or a coordinator notifying other vendors.

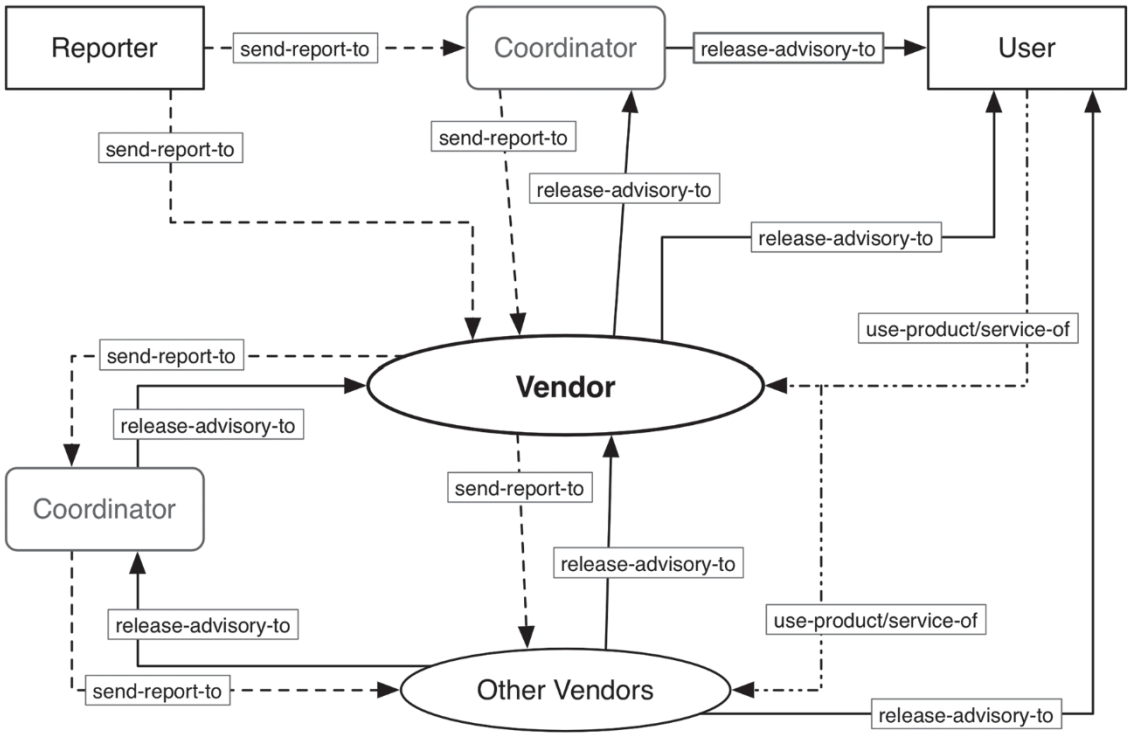


Figure 3 — Vulnerability information exchange

5.8 Confidentiality of exchanged information

5.8.1 General

Since vulnerability information can be used to attack vulnerable systems, sensitive vulnerability information should be communicated confidentially, particularly when the information is not publicly available.

5.8.2 Secure communications

Vendors should provide secure confidential methods for reporters to report vulnerability information. Message integrity is also important, particularly in verifying that remediation information is authentic. Common cryptographic protocols and implementations such as TLS, S/MIME, and OpenPGP can provide confidentiality and integrity. If there are other security requirements,ISO/IEC 27010[2] can be relevant. An example would be if a coordinator offers a reporter anonymity service.

5.9 Vulnerability advisories

Vulnerability information is generally published in an advisory. The advisory describes the vulnerability, usually focusing on remediation and mitigation, but can also include information about affected systems, threats, impact, and references. Users reading an advisory need sufficient information to make informed risk decisions about how to remediate or mitigate the vulnerability.

Publishing vulnerability advisories is described in Clause 7.

5.10 Vulnerability exploitation

In general, attackers seek to exploit vulnerabilities for some gain, almost always causing loss to users. Various factors such as target population, exposure of targets, value of targets to the attacker, and cost of exploit development, can influence whether or not a vulnerability will be exploited by attackers. Any attempt, however, to predict whether or not a vulnerability will or has already been used in attacks can be subject to considerable uncertainty. The most conservative assumption is that a vulnerability can and will (and can have already been) used in attacks.

5.11 Vulnerabilities and risk

Vulnerabilities contribute to risk, particularly when exploited in attacks. Vulnerability disclosure informs stakeholders about vulnerabilities and ideally includes remediation information, leading to fixed vulnerabilities and reduced risk. Vulnerability disclosure itself creates risk, since public disclosure provides information for exploit developers and attackers. The theory supporting vulnerability disclosure holds that the short-term risk caused by public disclosure is outweighed by longer-term benefits from fixed vulnerabilities, better informed defenders, and systemic defensive improvements.

6 Receiving vulnerability reports

6.1 General

This clause provides guidance for vendors on receiving information about potential vulnerabilities. A capability to receive vulnerability reports helps vendors more quickly become aware of new reports and establish working relationships with reporters and other stakeholders.

6.2 Vulnerability reports

6.2.1 General

Reporters notify vendors of potential vulnerabilities. Reports typically include a description of what product or service is affected, how the potential vulnerability can be identified, demonstrated, or reproduced, and what type of functional impact the vulnerability allows.

Reports may include proof-of-concept (PoC) code that demonstrates exploitation of the vulnerability. Since a vulnerability report is likely to contain sensitive, non-public information, vendors should provide mechanisms to receive reports confidentially (see 5.8 and 6.7).

6.2.2 Capability to receive reports

Vendors shall provide one or more technically current and usable mechanisms to receive reports of potential vulnerabilities. This corresponds to the receipt phase described in 5.6.3. Typical reporting mechanisms include:

— web forms;

— bug or issue tracking systems;

— vulnerability reporting services;

— e-mail, possibly an alias, list, or role address that is independent of any one individual.

Vendors should prefer secure mechanisms to receive reports, but may accept reports through less secure mechanisms such as plaintext e-mail or public bug tracking systems.

To facilitate the verification step of the vulnerability handling process, vendors should design reporting mechanisms to elicit information useful in assessing the validity, severity, scope, and impact of vulnerabilities. Such information includes:

— product or service name and affected versions;

— class or type of vulnerability, optionally using a taxonomy like CWE;

— possible root cause;

— PoC code or other substantial evidence;

— tools and steps to reproduce the vulnerable behaviour;

— impact and severity estimate;

— scope assessment, other products, components, services, or vendors thought to be affected;

— disclosure plans, specifically embargo and publication timelines.

For further examples of information to request in a report, see Annex B.

6.2.3 Monitoring

Vendors shall monitor their reporting mechanisms for new reports and communications related to existing reports. In addition, vendors should monitor public sources (including mailing lists and social media used by the security research community) for reports of vulnerabilities. Vendors should also monitor customer service and support and other organizational communications channels that are likely to receive vulnerability reports.

6.2.4 Report tracking

Vendors should use a mechanism to label (assign identifiers to) and track reports, for example, bug tracking, CRM, or ticketing systems. Vendors should provide reporters and other stakeholders with vulnerability report identifiers. Vendors may use more than one labelling and tracking mechanism, however, multiple mechanisms can cause confusion.

Other stakeholders can also use labelling and tracking mechanisms.

6.2.5 Report acknowledgement

Vendors shall acknowledge receipt of potential vulnerability reports within 7 calendar days.

The response can be automated, but should be meaningful. The response should include a tracking number or identifier, and preliminary status information. The response can indicate that the report is under investigation, or requires further information, or is considered to be incomplete, spurious, or otherwise irrelevant.

In the case of significantly inaccurate, repeated, or spurious reports, no response is necessary, or an automated response is acceptable.

The initial acknowledgement from vendor to reporter is important in establishing a working relationship. Many reporters become frustrated by the inability to report to vendors or the lack of response from vendors. Frustrated reporters are more likely to seek other means of disclosure, including public disclosure[14].

Most of the remediation development process is not visible to the reporter. It is therefore important to communicate realistic expectations and status updates to reporters.

6.3 Initial assessment

Vendors shall perform initial assessment, or triage, of vulnerability reports. This corresponds to the Verification phase described in 5.6.4. Reports can be prioritized and categorized based on severity, impact, scope, ease of exploitation, likelihood of independent discovery, and other factors.

This initial assessment phase can be tedious and time consuming. New reports should be examined carefully enough to minimize false negatives. That is, the initial assessment should be designed to have high sensitivity, correctly identifying and rejecting reports that are not vulnerabilities at the cost of accepting reports that later turn out not to be vulnerabilities. New reports should also be compared with existing reports to identify duplicates.

At this phase, vendors should take significant care to only reject reports that are strongly considered not to be vulnerabilities and do not warrant further response. In such cases, the reporter should be informed of the vendor’s assessment.

If a vendor does not consider a report to be a vulnerability, the vendor shall inform the reporter and other stakeholders.

6.4 Further investigation

For reports that require further investigation or are considered to be valid vulnerabilities, vendors shall begin vulnerability handling processes. As noted in Figure 1, these processes are described in ISO/IEC 30111. Investigation and vulnerability handling correspond to the remediation development phase described in 5.6.5.

In order to perform further investigation, vendors may communicate with reporters and other internal and external stakeholders to understand the vulnerability and its impact. Vendors should request additional information from reporters as needed to fully assess or reproduce the reported vulnerability.

If other vendors are affected or likely to be affected, the initial vendor should notify the other vendors or engage a coordinator. Vendors should be aware of supply chain relationships and common usage of shared or similar components, such as libraries, protocols, and formats.

6.5 On-going communication

During vulnerability handling, vendors shall communicate with reporters and other stakeholders. Such communication should include information such as:

— status updates;

— significant new information;

— changes to existing plans;

— disclosure timing.

When there is a disagreement among stakeholders, particularly concerning public disclosure, vendors should communicate their intentions so that stakeholders are not surprised.

Supply chain relationships, or the need to involve other stakeholders during the investigation, can introduce additional delays in communications. When necessary, vendors should explain communication and process delays to stakeholders.

6.6 Coordinator involvement

Coordinators can be involved in the receiving phase. Coordinators can act as reporters, or on behalf of reporters, attempting to identify and report vulnerabilities to vendors. Coordinators can mediate between reporters and vendors. Coordinators can also provide additional support in assessing the validity, severity, impact, and scope of vulnerabilities.

Coordination is described further in Clause 8.

6.7 Operational security

Vendors should consider operational security throughout the processes of receiving and communicating about vulnerability reports.

Reporting mechanisms (see 6.2) and on-going communications (see 6.5) should provide confidentiality to limit access to sensitive, non-public vulnerability information. Reporting and communication mechanisms may also provide authentication. Reporting mechanisms should provide the ability for reporters to verify the identity of the vendor.

Typical security mechanisms include:

— web-based forms or applications using TLS (HTTPS);

— e-mail encryption and signing using S/MIME or OpenPGP.

Vendors should also consider internal operational security and limit access to non-public vulnerability information to staff and organizational units that need to know.

7 Publishing vulnerability advisories

7.1 General

This clause provides guidance on disclosing vulnerability information to users, other stakeholders, and the public. In most cases, at this phase, vendors have developed and tested a remediation for the vulnerability, having followed the processes described in ISO/IEC 30111. In most cases, vendors should publish, or publicly disclose, information about identifying and remediating the vulnerability. Publishing advisories generally corresponds to the Release phase described in 5.6.6.

7.2 Advisory

The term advisory is used broadly to mean any document or message containing vulnerability information. Advisories should be intended for widespread, usually public disclosure (publication) and should enable users to identify vulnerable products and services and take action to remediate vulnerabilities. Advisory authors should consider the needs of the intended audience and produce advisories that are effective in terms of informational content, distribution mechanisms, and presentation format.

Example advisories can be found in Annex C.

7.3 Advisory publication timing

Vendors should work to balance risk while choosing when to publish advisories. To reduce disruptions to users, vendors may publish advisories in batches and schedule releases in advance. Vendors may also publish advisories as soon as corresponding remediations are available.

If a vulnerability is being actively exploited and remediation is not available, vendors should publish advisories informing users of the current threat and what steps users can take to reduce risk until a remediation is available.

Vendors should, when possible, attempt to coordinate advisory release in instances where their products are affected by interrelated vulnerabilities. Releasing information about a vulnerability in one product can expose other interdependent products to increased risk of attack. This situation typically occurs when a software library, protocol, module or other component is used in multiple products or services, often affecting multiple vendors. It is possible that a coordinator can facilitate disclosure and advisory publication timing among multiple vendors.

Other factors to consider include:

— any embargo periods (see 5.6.8);

— expected time between publication and remediations being applied (see 5.6.6);

— reporter’s agenda for publication;

— advisory release schedule of other vendors;

— possible negative side-effects of a workaround or remediation;

— language localization;

— readiness of remediation for different versions or platforms;

— readiness of customer support and sales organizations.

7.4 Advisory elements

7.4.1 General

Advisories should contain sufficient information to enable the target audience — including system administrators, developers, managers, and users — to decide if the vulnerabilities are relevant and how to remediate them.

Readers of advisories have different needs that can be dependent on market segment or regulatory requirements. Technical users such as system administrators tend to prefer detailed information about vulnerabilities and workarounds. Consumers typically appreciate information on how to determine if they are using the affected products and plain, easily understood remediation advice. Vendors should design advisories for the expected audience. A single advisory can address multiple vulnerabilities, for example, when a single remediation resolves multiple vulnerabilities.

The following subclauses describe the elements included in advisories. The list is not exhaustive and vendors may include additional elements. Unless otherwise stated, the order of the subclauses does not indicate the order of elements appearing in an advisory.

7.4.2 Identifiers

Advisories shall contain certain identifiers.

a) Advisory identifier: An advisory shall be labelled with a unique and consistent identifier for the advisory document. CVE identifiers may be used as advisory identifiers if a single advisory describes only one vulnerability. To the extent possible, CVE identifiers are assigned for individual vulnerabilities. A single advisory can address multiple vulnerabilities.

b) Vulnerability identifier: An advisory shall provide unique and consistent identifiers for vulnerabilities addressed in the advisory. Identifiers should be sufficiently unique and consistent so as to not confuse different advisories or vulnerabilities. Advisory authors should choose a common, shared vulnerability identification system such as CVE.

c) Product identifiers: An advisory should include product name and version information in order to inform readers which products are affected and optionally which products are not affected. See 7.4.6.

7.4.3 Date and time

Advisories shall indicate the date of initial publication and may include other dates, for example, as part of the revision history. Advisories shall use unambiguous date and time references and should use ISO 8601[8].

7.4.4 Title

The title of an advisory should contain a reference to a product or some other description that is informative to readers so that they can quickly decide if the advisory is relevant.

7.4.5 Overview

The overview element provides a brief, high-level summary of the vulnerability so that users can understand the salient points of the report and quickly determine if the advisory is applicable to their environment.

7.4.6 Affected products

The advisory shall provide sufficient information for users to determine if they are affected by the vulnerability or not.

This element of the advisory provides a list of known, supported, and affected products and their versions. This element may provide instructions about how to verify the version of the product. In most cases, services do not have version identifiers but can have a date when the last update or change was made.

This element may optionally note products and versions that are no longer supported or are not affected by the vulnerability.

Information useful in describing affected products can include:

— product names, including common or historical names;

— version numbers or strings;

— file hashes;

— PoC code to safely test for the existence of the vulnerability.

7.4.7 Intended audience

Advisory authors should consider their intended audience when developing and producing the advisory. Typically, the audience will be users who are responsible for identifying vulnerable systems and performing remediation. Advisories may provide sections intended for specific audiences, for example, different remediation advice for developers, system administrators, or end users. Audience-specific language in an advisory is optional.

7.4.8 Localization

Vendors can provide advisories with appropriate language and localization selections.

7.4.9 Description

The advisory should provide sufficient information that users can establish if they are affected and to assess their exposure. At the same time, the advisory should not provide too much detail in order to avoid making exploiting the vulnerability easier.

Advisories may describe the class or type of vulnerabilities, for example using the CWE taxonomy.

7.4.10 Impact

The advisory should describe the potential impact or consequence of the vulnerability if it is exploited. The impact should at a minimum explain the direct technical behaviour that the

vulnerability allows. The impact can describe security violations, access or privilege gains, likely subsequent impacts, and common attack scenarios.

The impact can be described using a model such as the CIA triad (confidentiality, integrity, and availability) or the Parkerian hexad (confidentiality, possession or control, integrity, authenticity, availability, and utility).

7.4.11 Severity

The advisory should provide a severity rating for each vulnerability to help users assess risk more quickly and programmatically. Advisory authors should consider existing systems such as CVSS, but may use other or develop their own systems. A severity rating system used in the advisory should be documented and the documentation referenced from the advisory.

7.4.12 Remediation

The advisory should provide information about what action affected users should take in order to remediate the vulnerability and reduce its impact. Remediation typically involves installation of an upgrade, patch, or new version.

As appropriate or necessary, the advisory should provide workarounds by which users can protect the affected product or service until a more permanent solution is implemented. Workarounds can include changing a product's configuration to restrict functionality and introducing a firewall to restrict network accessibility.

7.4.13 References

References to additional or related information may be added in this element. Examples of such references can be links to related advisories published by other parties or a reference to a CVE identifier. It is important to refer to original or source material and common cross-references such as CVE.

7.4.14 Credit

In this element, a vendor should acknowledge a reporter for reporting the vulnerability and being cooperative during the process, if the reporter wishes to be publicly credited. This is an optional element.

7.4.15 Contact information

The advisory should provide contact information so that readers of the advisory can contact the vendor.

7.4.16 Revision history

This element should contain the date when the advisory was first published. It may contain a modification history if the advisory is subsequently updated.

7.4.17 Terms of use

The advisory should provide information about copyright and terms of use and redistribution of the advisory.

7.5 Advisory communication

Vendors should establish and maintain appropriate methods for communicating advisories to their users. Common methods include web sites, mailing lists, feeds, and automatic update mechanisms. Each vendor may determine the best method as it applies to their user community. Vendors may also choose to post advisories to public vulnerability discussion forums to share their information with a wider audience.

Vulnerability databases monitor public disclosures and collect vulnerability reports. Contacting a database directly, disclosing in a monitored forum, or providing a stable and consistent distribution channel can lead to inclusion in vulnerability databases.

7.6 Advisory format

Advisories should be formatted consistently and in a manner that clearly conveys important information. Changes to the format will likely require readers to change tools and processes used to consume advisories. Therefore, changes should be made infrequently.

Advisory authors should consider providing the content in both human- and machine-readable formats such as CVRF. Machine-readable advisory formats should be documented.

7.7 Advisory authenticity

Vendors shall provide the ability to authenticate and verify the integrity of advisories. This can be accomplished by cryptographically signing the advisory. Accepting a counterfeit advisory and acting on it can cause systems to be compromised. Depending on the cryptographic technique used, a vendor should publish required cryptographic material or credentials (e.g. public keys or certificates).

7.8 Remediations

7.8.1 General

A primary purpose of advisories is to document remediations (see 7.4.10). An advisory may describe remediation activities. A remediation often takes the form of a software change.

7.8.2 Remediation authenticity

If users are required to take action to apply a remediation, then vendors shall provide the ability to authenticate and verify the integrity of remediations. Typically, this is implemented as digital signatures of software updates.

7.8.3 Remediation deployment

The mechanism used to deploy remediations should be tailored to match user needs and the way a product is operated in the field. Vendors should consider providing automatic update deployment systems that require limited or no user interaction. Vendors should provide a method to control the automatic update deployment systems if appropriate. Remediation deployment corresponds to the Release phase described in 5.6.6.

8 Coordination

8.1 General

Coordinators may play multiple roles in vulnerability disclosure, for example:

— act as a trusted liaison between involved parties;

— coordinate advisory public release dates;

— enable communication between primary stakeholders (vendors and reporters);

— enable controlled disclosure to other stakeholders (such as CSIRTs);

— provide experience and guidance to disclosure processes;

— provide domain-specific expertise;

— support and facilitate collaboration among stakeholders.

Coordinators should set appropriate expectations about the services and levels of support they provide. The choice of a coordinator may depend on such factors as geographical proximity, language and acceptable operation model.

In cases when there are multiple vendors affected by a vulnerability, vendors should attempt to coordinate the timing of release of their advisories, either directly or with the assistance of a coordinator. A vendor may request that the coordinator provide or obtain a CVE identifier. In some cases, more than one coordinator can be involved. Vendors may suggest that one coordinator act as a leader in order to reduce complexity and confusion.

8.2 Vendors playing multiple roles

8.2.1 General

After investigating a reported vulnerability, a vendor can find the need to act in the role of coordinator, reporter, or both. If a vulnerability is caused by some component or underlying platform which another vendor supplies, the initial vendor may act as a reporter or coordinator. In addition, vendors sometimes encounter situations where it is desirable for them to report vulnerabilities to other vendors, causing them to act in the role of a vulnerability reporter. This subclause describes how such vulnerability reporting among vendors should be carried out.

8.2.2 Vulnerability reporting among vendors

Typical cases when a vendor may report vulnerability information to other vendors include:

— when the vendor believes that a vulnerability in their product or service is caused by a component or a tool which they are licensed to use by the second vendor;

— when a vulnerability is identified with a new methodology or insight and many of other vendors' products and services of the same category are also believed to be vulnerable; or

— when a vulnerability is identified in a protocol or format supported by other vendors' products or services.

It may not always be possible for a vendor, reporter, or coordinator to identify all of the other affected vendors. Even in cases where the vendor can be identified, it may not be possible to identify an appropriate point of contact. Such cases can benefit from the involvement of a coordinator who can provide additional support to vendor contact and notification efforts.

8.2.3 Reporting vulnerability information to other vendors

A vendor can report vulnerability information to other vendors directly or indirectly through coordinators in the same manner that a reporter reports a potential vulnerability to a vendor. In this case, the initial vendor can also inform the other vendor when the vulnerability is interrelated with the initial vendor's product or service and request the other vendor provide remediation before public disclosure so that all the vendors involved can synchronize the disclosure.

9 Vulnerability disclosure policy

9.1 General

To convey intentions and expectations, vendors shall develop and publish an external vulnerability disclosure policy. Alternatively, a vendor may reference and adhere to an existing published policy. The policy shall contain the required elements in 9.2. The external policy is meant for reporters, users, and other stakeholders. A vendor may also create a corresponding internal policy. The internal policy is meant for employees or agents performing vulnerability disclosure for the vendor. The two policies should agree. The internal policy can contain further details, private information, and processes that are needed for internal reasons and to meet the external policy.

Each vendor has different requirements and resources available for dealing with security vulnerability information. Vendors should develop policy before engaging in vulnerability disclosure. Developing a policy is part of the Preparation phase described in 5.6.2. The disclosure policy should state the intentions of the vendor, its responsibilities as well what the vendor expects from other stakeholders. The vulnerability disclosure policy should be simple and clear to facilitate easy reporting of vulnerabilities to the vendor. Vendors should consider intuitive placement of their disclosure policy and other relevant information. One such location can be a security web page (e.g., www.example.com/security).

9.2 Required policy elements

9.2.1 General

A vulnerability disclosure policy shall include the following elements.

9.2.2 Preferred contact mechanism

The provisions in 6.2.1 require that vendors provide one or more technically current and usable mechanisms to receive reports. Vendors shall include information about these contact mechanisms in the vendor's vulnerability disclosure policy.

Contact mechanisms can include one or more of the following:

a) e-mail address. Examples of e-mail aliases that can be used include the following:

   — security-alert@example.com;

- security@example.com;
- secure@example.com;
- psirt@example.com;
- csirt@example.com;

b) phone number;

c) web form. Advantages of this mechanism include greater ability to influence the content of reports (e.g., the vendor can distinguish between optional and mandatory information) and better integration with a vulnerability report database;

d) contact information for customer service, if customer service is trained to receive vulnerability reports.

9.3 Recommended policy elements

9.3.1 General

A vulnerability disclosure policy should include the following elements.

9.3.2 Vulnerability report contents

A vendor can wish to elicit information that might be helpful to understanding the vulnerability and possible remediation and mitigation. A vendor can provide a form for this purpose (see 6.2.1).

In cases when a vulnerability affects multiple vendors, it is useful for vendors to know if the reporter has also reported the vulnerability to the other affected vendors.

9.3.3 Secure communication options

Vendors should provide a secure communications channel using technologies such as TLS, S/MIME, or OpenPGP. If a vendor provides a web-based reporting mechanism, that mechanism shall use TLS (HTTPS) or an equivalent, widely-used cryptographic system that protects the confidentiality of submissions and authenticates the web site. Vendors should configure these capabilities prior to communication with reporters.

9.3.4 Setting communication expectations

Vendors should set expectations for communication, including initial acknowledgement and status updates. Vendors should provide updates to the reporter using the agreed method of communication.

It is important that vendors maintain open and cooperative dialogue with reporters so that information about vulnerabilities can be shared and risk for users can be reduced as efficiently as possible. If the vendor determines that the reporter has not provided enough information, the vendor may contact the reporter to request additional details. Vendors acting as reporters or coordinators communicate with other vendors in their supply chains. The policy should support all of these communications possibilities.

In most cases, the team dealing with vulnerability reports is not able to deal with security incidents and other security related questions. The policy may specify contact points for these other types of requests.

The policy may describe the mechanisms used to track reports and communications with reporters and other stakeholders.

9.3.5 Scope

Vendors should describe which products and services are eligible to receive remediations. Vendors should also describe which products and services are not eligible to receive remediations. For example, a product can be in a test phase or no longer supported.

9.3.6 Publication

Vendors should describe how advisories and remediations are distributed.

9.3.7 Recognition

Vendors should describe how reporters are recognized for their efforts. Recognition can include credit in advisories, gifts, and bounty payments.

9.4 Optional policy elements

9.4.1 General

A vulnerability disclosure policy may contain the following elements.

9.4.2 Legal considerations

The act of finding or reporting a vulnerability can violate law or other regulation. Vendors can consider not taking legal action against reporters who voluntarily, in good faith, report vulnerabilities.

9.4.3 Disclosure timeline

Vendors can publish expected timelines for response and disclosure.

Annex A
(informative)
Example vulnerability disclosure policies

A.1 Facebook

https://www.facebook.com/whitehat [1]

A.2 CERT/CC

https://www.cert.org/vulnerability-analysis/vul-disclosure.cfm [1)]

A.3 Zero Day Initiative

http://www.zerodayinitiative.com/advisories/disclosure_policy/ [1)]

A.4 Cisco

http://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html [1)]

A.5 NCSC-FI

https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices/vulnerabilitycoordination.html [1)]

https://www.viestintavirasto.fi/attachments/vulncoord/68RKIxXES/Vulncoord_policy_1.1.pdf [1)]

A.6 NCSC-NL

https://www.ncsc.nl/english/security [1)]

https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html [1)]

https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/news/responsible-disclosure-guideline/1/Responsible%2BDisclosure%2BENG.pdf [1)]

A.7 Rapid7

https://www.rapid7.com/disclosure/ [1)]

[1] Retrieved on 2017-05-18.

Annex B
(informative)
Information to request in a report

The information to request from reporters differs based on the vendor's specific choices and the affected product or service.

The following information can be useful when submitting a report to a vendor:

a) product or service name, URL, or affected version information;

b) operating system of involved components;

c) version information;

d) technical description of what actions were being performed and the result in as much detail as possible;

e) sample code that was used to test or demonstrate the vulnerability;

f) reporter's contact information;

g) other parties involved;

h) disclosure plans;

i) threat/risk assessment details of the identified threats and/or risks including a risk level (high, medium, low) for assessment result;

j) software configuration of the computer or device configuration at time of discovering the vulnerability;

k) relevant information about connected components and devices if vulnerability arises during interaction. When a secondary component or device triggers the vulnerability, these details should be provided;

l) time and date of discovery;

m) browser information including type and version information.

Annex C
(Informative)
Example advisories

C.1 Example advisory

This example describes a fictitious vulnerability affecting a fictitious product and vendor.

ROB-2017-004: Robotron R.U.R processors vulnerable to flying insects

Date

2016-11-25

Overview

A vulnerability has been discovered in the R.U.R processor models 48, 49 and 51 of the Robotron mainframe. This vulnerability can be used to elevate process execution privilege.

This vulnerability is assigned CVE ID CVE-2016-000111. Internal Bug ID is RT12345.

The full text of this advisory can be found at <https://www.robotron.example.com/advisories/ROB-2017-004.html>. All advisories published by Robotron Corporation and their SHA-512 hashes are available at <https://www.robotron.example.com/advisories/>. The SHA-512 hash of this advisory is ABCDEF123456567890.

Affected products

The following Robotron mainframes models are affected by this vulnerability:

— Model 1;
— Model 2;
— Model 2a;
— Model 4.

The following Robotron mainframes models are not affected by this vulnerability:

— Model 3;
— Model 5.

No other Robotron products are affected by this vulnerability.

How to verify if the product is affected

To verify if your mainframe is affected by this vulnerability perform the following steps.

1) Shut down to operating system.
2) Disconnect power from the CPU rack.
3) Open the rear panel of the CPU rack.
4) Locate the processor board. By default, it is located in the first slot from the left. The processor board is marked by the word “CPU” on the edge.
5) Unplug the board and examine the upper right corner. It should contain the model and HW revision of the processor.

Your mainframe is affected by this vulnerability if the processor model is “R.U.R” and HW revision is one of the following: 48, 49 or 51.

Vulnerability description

This vulnerability can be triggered by a flying insect approximately 7 mm long. Such insect can electrically connect wires on the processor board. Connecting wires will indicate to the processor that the currently executing process must be given superuser privileges.

This cannot be accomplished by non-flying insects as exposed power leads on the edge of the processor board will prevent such insect from reaching the area in question (positioned towards the middle of the board).

Impact

By exploiting this vulnerability, it is possible to elevate privileges of a process that is currently executing. After elevating privileges, the process can execute commands as a superuser and modify any aspect of the mainframe.

Severity

The CVSSv3 scores for this vulnerability are: 6.4 (Base) and 5.8 (Temporal)

CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Remediation

The workaround for this vulnerability is not to allow flying insects into the mainframe room (i.e. keep windows and doors closed).

To remediate this vulnerability, users should download the firmware from the R.U.R. support web page at URL. Instructions how to install the firmware are included at the same web page.

After downloading the firmware users should verify that SHA-512 hash matches the one published on the support page.

Do not install firmware whose hash does not matches the published one. In such instance immediately notify Robotron Support Service of the problem.

Credit

This vulnerability is independently discovered by Grace Hooper and Ada Lovelace.

Contact information

Customers and users of Robotron equipment should report all potential security vulnerabilities to psirt@robotron.example.com. All reports will be acknowledged within 48 hours.

For non-security issues customers should contact Robotron Support Service via e-mail at service@robotron.example.com or call a telephone number listed at <https://www.robotron.example.com/contact.html>.

Revision history

Version	Date	Comments
1.0	2016-11-04	Initial publication
1.1	2016-11-11	HW revision 51 is identified as vulnerable. The previous version of this advisory is available at <URL-rev1.0>

Terms of use

This advisory can be freely distributed in its entirety or in parts providing that the original advisory URL is included. The URL must not point to a non-Robotron site. Robotron corporation does not […]

C.2 Heap memory corruption in ASN.1 parsing code generated by Objective Systems Inc. ASN1C compiler for C/C++

https://github.com/programa-stic/security-advisories/tree/master/ObjSys/CVE-2016-5080 [2]

C.3 Multiple Vulnerabilities in Network Time Protocol Daemon Affecting Cisco Products: November 2016

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161123-ntpd 2)

C.4 RHSA-2017:0057 — Security Advisory

https://access.redhat.com/errata/RHSA-2017:0057 2)

C.5 Alert (TA10-159A) Adobe Flash, Reader, and Acrobat Vulnerability

https://www.us-cert.gov/ncas/alerts/TA10-159A 2)

[2] Retrieved on 2017-05-18.

Annex D
(informative)
Summary of normative elements

Subclause	Normative element
5.3.1 ISO/IEC 30111	ISO/IEC 30111 shall be used in conjunction with this document.
6.2.1 Capability to receive reports	Vendors shall provide one or more technically current and usable mechanisms to receive reports of potential vulnerabilities.
6.2.2 Monitoring	Vendors shall monitor their reporting mechanisms for new reports and communications related to existing reports.
6.2.4 Report acknowledgement	Vendors shall acknowledge receipt of potential vulnerability reports within 7 calendar days.
6.3 Initial assessment	Vendors shall perform initial assessment, or triage, of vulnerability reports. If a vendor does not consider a report to be a vulnerability, the vendor shall inform the reporter and other stakeholders.
6.4 Further investigation	For reports that require further investigation or are considered to be valid vulnerabilities, vendors shall begin vulnerability handling processes.
6.5 On-going communication	During the course of vulnerability handling, vendors shall communicate with reporters and other stakeholders.
7.4.2 Identifiers	Advisories shall contain certain identifiers: a) Advisory identifier: An advisory shall be labelled with a unique and consistent identifier for the advisory document; b) Vulnerability identifier: An advisory shall provide unique and consistent identifiers for vulnerabilities addressed in the advisory.
7.4.3 Date and time	Advisories shall indicate the date of initial publication and may include other dates, for example, as part of the revision history. Advisories shall use unambiguous date and time references and should use ISO 8601.
7.4.6 Affected products	The advisory shall provide sufficient information for users to determine if they are affected by the vulnerability or not.
7.7 Advisory authenticity	Vendors shall provide the ability to authenticate and verify the integrity of advisories.
7.8.2 Remediation authenticity	If users are required to take action to apply a remediation, then vendors shall provide the ability to authenticate and verify the integrity of remediations.

Subclause	Normative element
9.1 General	To convey intentions and expectations, vendors shall develop and publish an external vulnerability disclosure policy. The policy shall contain the required elements in 9.2.
9.2.1 General	A vulnerability disclosure policy shall include the following elements.
9.2.2 Preferred contact mechanism	Vendors shall include information about these contact mechanisms in the vendor's vulnerability disclosure policy.
9.3.3 Secure communication options	If a vendor provides a web-based reporting mechanism, that mechanism shall use TLS (HTTPS) or an equivalent, widely-used cryptographic system that protects the confidentiality of submissions and authenticates the web site.

Bibliography

[1] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

[2] ISO/IEC 27010, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*

[3] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on* ISO/IEC 27002 *for cloud services*

[4] ISO/IEC 27034 1, *Information technology — Security techniques — Application security — Part 1: Overview and concepts*

[5] ISO/IEC 27034 5, *Information technology — Security techniques — Application security — Part 5: Protocols and application security controls data structure*

[6] ISO/IEC 27035 1, *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*

[7] ISO/IEC 27036 3, *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security*

[8] ISO 8601, *Data elements and interchange formats — Information interchange — Representation of dates and times*

[9] ITU-T X.1520, *Common vulnerabilities and exposures*

[10] ITU-T X.1521, *Common vulnerability scoring system*

[11] ITU-T X.1524, *Common weakness enumeration*

[12] COMMON V.R.F. (CVRF). *Industry Consortium for Advancement of Security on the Internet* (ICASI). *Available at* < https://www.icasi.org/the-common-vulnerability-reporting-framework-cvrf-v1-1/ >

[13] COMMON V.R.F. (CVRF). OASIS *Common Security Advisory Framework* (CSAF) TC. *Available at* < https://www.oasis-open.org/committees/csaf/charter.pdf >

[14] *Vulnerability Disclosure Attitudes and Actions*. NTIA *Multistakeholder Process: Cybersecurity Vulnerabilities*. *Available at* < https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf >

[15] ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security*

[16] ISO/IEC 18405, *Information technology — Security techniques — Methodology for IT security evaluation*

Informasi pendukung terkait perumus standar

[1] Komite Teknis Perumus SNI

Komite Teknis 35-04 Keamanan Informasi, Keamanan Siber, dan Perlindungan Privasi

[2] Susunan Keanggotaan Komite Perumus SNI

Ketua : Soetedjo Joewono
Sekretaris : Didik Utomo
Anggota :
1. Bety Hayat Susanti
2. Bisyron Wahyudi
3. Chandra Yulistia
4. Pedro Libratu Putu Wirya
5. Pratama Dahlian Persadha
6. Sari Agustini Hafman
7. Sarwono Sutikno
8. Satrio Wibowo
9. Sugi Guritman
10. Wisnoe Pasetyo Pribadi
11. Zaenal Arifin

[3] Konseptor Rancangan SNI

Gugus Kerja 3 Evaluasi, Pengujian dan Spesifikasi Keamanan – Komtek 35-04:

Ketua : Bisyron Wahyudi
Wakil Ketua : Zaenal Arifin
Sekretaris : Yhufi Swastantri Gustiviana
Anggota :
1. Adang Rochiyat
2. Bangkit Hardiawan
3. Endro Ariyanto
4. Faizal Achmad
5. Is Esti Firmanesa
6. Magdalena Christine
7. Mohamad Rahmadi

[4] Sekretariat Pengelola Komite Teknis Perumus SNI

Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi
Badan Siber dan Sandi Negara (BSSN)