INSO

21078

1st.Edition

2016

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران

۲۱۰۷۸

چاپ اول

۱۳۹۵

فناوری اطلاعات-

فنون امنیتی-فرایندهای ساماندهی آسیب‌پذیری

Information technology — Security techniques — Vulnerability handling processes

ICS: 35.040

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و کسب‌وکار است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها واسط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و الزامات خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، پیاده‌سازی بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، پیاده‌سازی استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد
«فناوری اطلاعات-فنون امنیتی-فرایندهای ساماندهی آسیب‌پذیری»

رئیس:	**سمت و/ یا محل اشتغال:**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار، فوق لیسانس مدیریت اجرایی)	مدیرکل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات
اعضاء: (اسامی به ترتیب حروف الفبا)	
ناظمی، اسلام (دکترای مهندسی کامپیوتر)	استادیار دانشگاه شهید بهشتی
نصیری آسایش، حمید رضا (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی
دوست‌محمدی، وحید (کارشناسی ارشد مهندسی صنایع گرایش فناوری اطلاعات)	کارشناس مرکز مدیریت راهبردی افتا
محمدیان، بهزاد (فوق لیسانس مهندسی برق)	کارشناس مرکز مدیریت راهبردی افتا
ابوالقاسمی، پیمان (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
ارجمند، مهدی (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
رادمهر، وحید (کارشناسی مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

جوادزاده، غزاله
(کارشناسی ارشد مهندسی کامپیوتر)
پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

مغانی،مهدی
(فوق لیسانس ریاضی کاربردی)
کارشناس تدوین استانداردهای حوزه فناوری اطلاعات
سازمان فناوری اطلاعات ایران

ویراستار:

قسمتی، سیمین
(کارشناسی ارشد مهندسی فناوری اطلاعات)
مشاور مرکز آپا دانشگاه تربیت مدرس

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات-فنون امنیتی-فرایندهای ساماندهی آسیب‌پذیری» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است، در چهارصد و بیست و هشتمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۵/۰۳/۰۸ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

منبع و مأخذی که برای تهیه و تدوین این استاندارد مورد استفاده قرار گرفته به توصیف زیر است:

ISO/IEC 30111:2013, Information technology — Security techniques — Vulnerability handling processes

مقدمه

این استاندارد ملی فرآیندهای ادارهٔ گزارش‌های آسیب‌پذیری‌های بالقوه را در محصولات و خدمات برخط برای عرضه‌کنندگان توصیف می‌کند.

مخاطب این استاندارد شامل مصرف‌کنندگان، توسعه‌دهندگان، عرضه‌کنندگان، و ارزشیابی‌کنندگان محصولات ایمن IT است. مخاطبان زیر ممکن است این استاندارد را استفاده کنند:

- توسعه‌دهندگان و عرضه‌کنندگان، هنگام پاسخ به آسیب‌پذیری‌های بالقوه یا واقعی گزارش‌شده؛
- ارزشیابی‌کنندگان، هنگام ارزیابی تضمین امنیتی فراهم شده با فرایندهای ساماندهی آسیب‌پذیری از سوی عرضه‌کنندگان و توسعه دهندگان و محصولات و خدمات مرتبط؛
- مصرف کنندگان، هنگام انتخاب محصول و عرضه‌کنندگان خدمت برخط برای بیان الزامات تضمین بهروش به توسعه‌دهندگان، عرضه‌کنندگان و تجمیع‌کنندگان.

این استاندارد ملی با استاندارد ISO / IEC 29147 [۵] ارتباط دارد. این استاندارد با عناصر شرح داده شده در در استاندارد ISO / IEC 29147 در نقطه‌ی دریافت گزارش‌های آسیب‌پذیری بالقوه، و در نقطه‌ی توزیع اطلاعاتِ برطرف نمودن آسیب‌پذیری واسطه دارد.

این استاندارد ملی عناصر مرتبط در بند 13.5 Flaw remediation در استاندارد ISO / IEC 15408-3، را در نظر می‌گیرد (ALC_FLR).

فناوری اطلاعات-فنون امنیتی-فرایندهای ساماندهی آسیب‌پذیری

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین و ارائه راهنماهایی برای چگونگی پردازش و برطرف نمودن[1] اطلاعات مربوط به آسیب‌پذیری‌های بالقوه در یک محصول یا خدمت برخط است.

این استاندارد ملی برای عرضه‌کنندگانی[2] که دست‌اندرکار ساماندهی آسیب‌پذیری‌ها هستند، کاربردپذیر است.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران به شماره ۲۷۰۰۰ سال: ۱۳۹۴، فناوری اطلاعات- فنون امنیتی- سیستم‌های (سامانه‌های) مدیریت امنیت اطلاعات - مرورکلی و واژگان

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف استاندارد ISO/IEC 27000، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

۳-۱

هماهنگ‌کننده[3]

مشارکت‌کننده‌ی اختیاری که می‌تواند به عرضه‌کنندگان و جستجوکنندگان در ساماندهی و افشای اطلاعات

1- Resolve
2- Vendors
3- Coordinator

آسیب‌پذیری یاری کند.

یادآوری ۱- به‌عنوان رابط مورد اعتماد بین طرف‌های دخیل عمل می‌کند و ارتباط بین طرف‌های دخیل (عرضه‌کنندگان و جستجوکنندگان) را توانمند می‌سازد.

۳-۲

خدمت برخط[1]

خدمتی که توسط سخت‌افزار، نرم‌افزار یا ترکیبی از این دو اجرایی می‌شود و از طریق یک شبکه یا خط ارتباطی فراهم می‌شود.

مثال: موتورهای جستجوگر، خدمات پشتیبانی برخط، رایانامه‌ای[2] که میزبان اینترنتی دارد، و نرم‌افزار به‌عنوان یک خدمت، به‌عنوان خدمات برخط در نظر گرفته می‌شوند.

۳-۳

محصول[3]

سامانه یا خدمتی که به‌منظور فروش یا ارائه رایگان، پیاده‌سازی یا پالایش می‌شود.

یادآوری ۱- در فناوری اطلاعات، اغلب بین محصولات نرم‌افزاری و سخت‌افزاری تمایز قائل می‌شوند، هرچند این مرز همیشه روشن نیست.

مثال : مسیریاب می‌تواند به‌عنوان یک سخت‌افزار دیده شود، گرچه، بخش حیاتی آن نرم‌افزار و/یا ثابت‌افزار[4] است.

۳-۴

ترمیم[5]

وصله[6]، تعمیر، ارتقا، پیکربندی یا تغییر مستندات به‌منظور پرداختن به آسیب‌پذیری است.

یادآوری ۱- تغییری به‌منظور رفع یا کاهش یک آسیب‌پذیری است. ترمیم اغلب در قالب تغییر پیکربندی، جایگزینی پرونده دودویی[7]، تغییر سخت‌افزار، یا وصله کد منبع، و غیره صورت می‌گیرد. ترمیم‌ها اغلب توسط عرضه‌کنندگان فراهم می‌شوند. عرضه‌کنندگان از اصطلاحات متفاوتی شامل به‌روزرسانی، وصله، تعمیر، تعمیر فوری[8]، و ارتقا استفاده می‌کنند.

1- Online service
2- Email
3- Product
4- Firmware
5- Remediation
6- Patch
7- Binary file
8- Hotfix

۳-۵

خدمت[1]

ابزار انتقال ارزش به کاربران از طریق تسهیل نتایجی که کاربران بدون مالکیت منابع یا مخاطرات مشخص، مایل به دست‌یابی به آن‌ها هستند.

۳-۶

سامانه[2]

ترکیب مولفه‌هایی که با هم در تعامل[3] هستند و برای رسیدن به یک یا چند هدف بیان‌شده سازماندهی شده‌اند.

[منبع: بند ۴-۳۱ استاندارد ISO/IEC 15288:2008]

۳-۷

عرضه‌کننده[4]

شخص یا سازمانی که محصول یا خدمت را توسعه داده یا مسئول حفظ آن است.

۳-۸

آسیب‌پذیری[5]

ضعف نرم‌افزار، سخت‌افزار، یا خدمت برخط که می‌تواند مورد بهره‌کشی[6] قرار گیرد.

[استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱]

یادآوری ۱- مثال‌های ضعف در یک سامانه، نقص‌های طراحی سخت‌افزار و نرم‌افزار، فرایندهای اداری ضعیف، نبود آگاهی و آموزش و پیشرفت‌ها در آخرین فناوری یا بهبودهایی در شیوه‌های جاری هستند. بدون در نظر گرفتن علت، بهره‌جویی از چنین آسیب‌پذیری‌هایی ممکن است موجب تهدیدهای واقعی برای سامانه‌های اطلاعاتی حیاتی-ماموریتی[7] شود.

۴ کوته‌نوشت‌ها

گروه پاسخگویی به رخداد مربوط به امنیت رایانه	Computer Security Incident Response Team	**CSRIT**

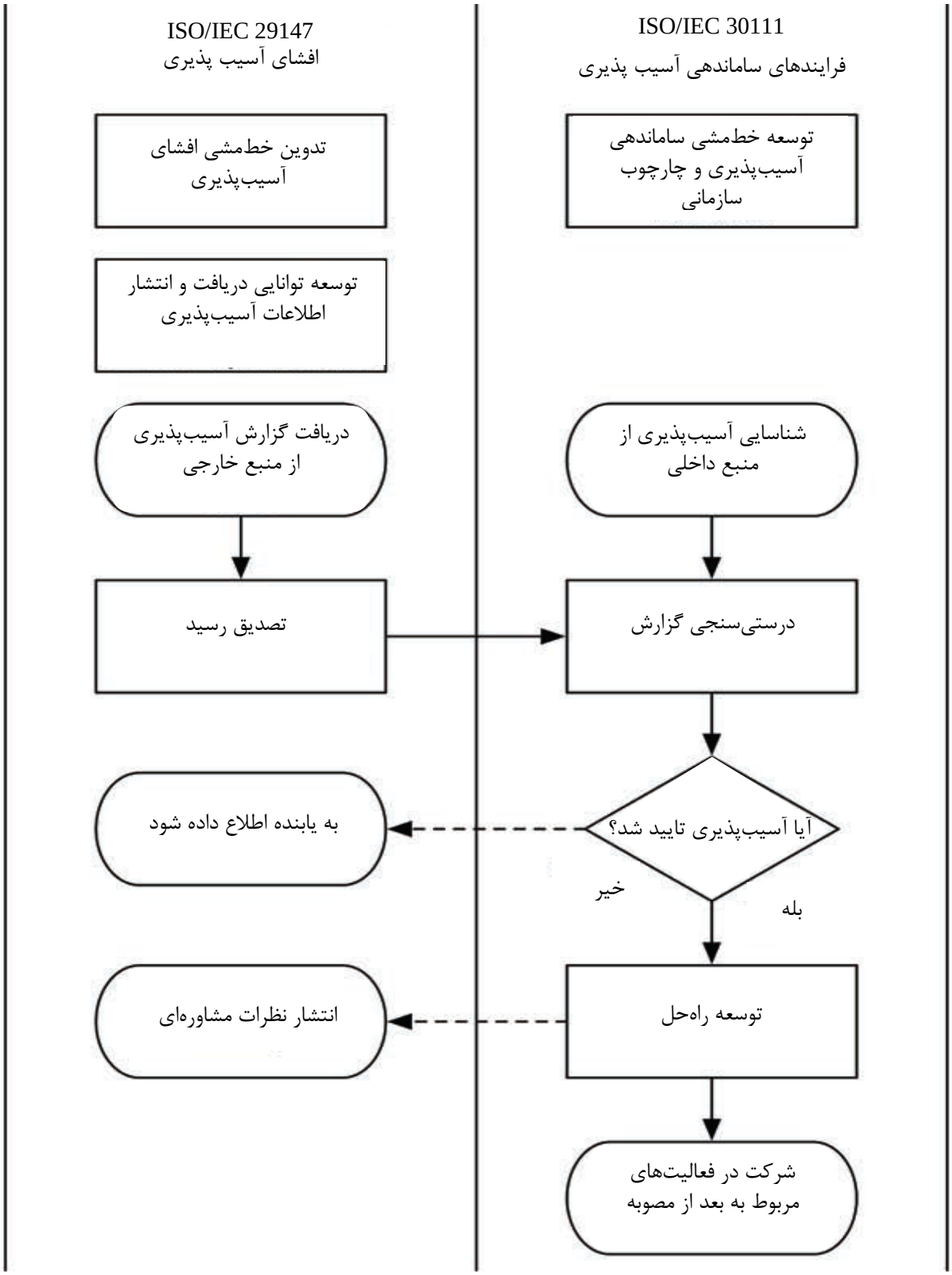
9- Service
1- System
2- interaction
3- Vendor
4 Vulnerability
5- Exploited
6- Mission-critical

گروه پاسخگویی به رخداد مربوط بـه امنیـت محصول	Product Security Incident Response Team	**PSRIT**

۵ واسط بین ISO/IEC 29147- افشای آسیب‌پذیری و ISO/IEC 30111- فرایندهای ساماندهی آسیب‌پذیری

همان‌گونه که در شکل ۱ نشان داده شده است، استاندارد ISO/IEC 29147- افشای آسیب‌پذیری و استاندارد ISO/IEC 30111- فرایندهای ساماندهی آسیب‌پذیری، مرتبط هستند. استاندارد ISO/IEC 29147 خط‌مشی‌هایی را برای عرضه‌کنندگان فراهم می‌آورد تا آن را در فرایندهای تجاری عادی[1] خود شامل کنند، این فرایندهای تجاری عادی شامل دریافت اطلاعات مربوط به آسیب‌پذیری‌های بالقوه از مردم و سازمان‌های خارجی و توزیع اطلاعات در مورد برطرف سازی آسیب‌پذیری‌ها در میان کاربران تحت تاثیر است. استاندارد ISO/IEC 30111 خط‌مشی‌هایی را برای چگونگی پردازش و برطرف نمودن اطلاعات مربوط به آسیب‌پذیری‌های بالقوه فراهم می‌آورد که این اطلاعات توسط افراد یا سازمان‌هایی که یک آسیب‌پذیری بالقوه را در یک محصول یا خدمت برخط کشف کرده‌اند، گزارش شده است. در حالی که استاندارد ISO/IEC 29147 به واسط بین عرضه‌کنندگان و افرادی که آسیب‌پذیری‌های بالقوه را کشف و گزارش می‌کنند، می‌پردازد، استاندارد ISO/IEC 30111 به بررسی، اولویت‌بندی و راه‌حل آسیب‌پذیری‌ها می‌پردازد، بدون توجه به این‌که منبع آسیب‌پذیری بالقوه بیرون از عرضه‌کننده بوده و یا این‌که داخل سازمان مربوط به عرضه‌کننده بوده است که معمولا شامل امنیت، توسعه، یا گروه‌های آزمون‌گر می‌شود.

1- Normal



شکل ۱- مدلی از واسط بین ISO / IEC 29147 **و** ISO / IEC 30111

۶ خط‌مشی و چارچوب سازمانی برای فرایندهای ساماندهی آسیب‌پذیری

۶-۱ کلیات

توصیه می‌شود عرضه‌کنندگان یک فرایند ساماندهی آسیب‌پذیری که مطابق با این استاندارد ملی باشد را ایجاد کنند برای بررسی و رفع آسیب‌پذیری‌های بالقوه آماده شوند. ایجاد یک فرایند ساماندهی آسیب‌پذیری کاری است که توسط یک عرضه‌کننده انجام می‌شود و توصیه می‌شود به‌صورت دوره‌ای مورد ارزیابی قرار گیرد تا فرصت‌های ارتقای فرایند را تسهیل کند و تضمینی ایجاد کند که فرایند، مطابق انتظار عمل می‌کند. توصیه می‌شود عرضه‌کنندگان رویه ساماندهی آسیب‌پذیری خود را مستندسازی کنند تا بتوان از تکرارپذیری آن اطمینان حاصل کنند. توصیه می‌شود مستندسازی رویه‌ها و روش‌های استفاده شده برای رهگیری آسیب‌پذیری‌های گزارش‌شده را توصیف کند.

برای دریافت اطلاعاتی در مورد چگونگی ریشه‌یابی علت یک آسیب‌پذیری (که خود یکی از گام‌های فرایند ساماندهی آسیب‌پذیری است و می‌تواند به ارتقای چرخه‌های زندگی توسعه‌ی امنیت نرم‌افزار کمک کند و منجر به توسعه یک محصول امن‌تر شود) به استاندارد ISO/IEC 27034 مراجعه شود. بند بعدی، مولفه‌هایی را توصیف می‌کند که توصیه می‌شود عرضه‌کنندگان آن‌ها را در فرایندهای ساماندهی آسیب‌پذیری خود شامل کنند.

۶-۲ توسعه خط‌مشی ساماندهی آسیب‌پذیری

توصیه می‌شود عرضه‌کننده، خط‌مشی ساماندهی آسیب‌پذیری را توسعه داده و حفظ کند تا مقاصد خویش هنگام بررسی و رفع آسیب‌پذیری‌ها برای توسعه فرایند ساماندهی آسیب‌پذیری را شفاف نموده و تعریف کند. توصیه می‌شود این خط‌مشی شامل دو بخش باشد: یک بخش فقط-درونی[1] و یک بخش عمومی.

بخش فقط-درونی خط‌مشی برای کارکنان عرضه‌کننده در نظر گرفته شده است و تعیین می‌کند که در هر یک از مراحل فرایند ساماندهی آسیب‌پذیری چه کسی مسئول است و توصیه می‌شود این افراد چگونه اطلاعات مربوط به آسیب‌پذیری‌های بالقوه را ساماندهی کنند. توصیه می‌شود این بخش شامل موارد زیر باشد:

الف- رهنمود اصلی[2]، اصول[3] و مسئولیت‌ها برای ساماندهی آسیب‌پذیری‌های بالقوه در محصولات یا خدمات برخط؛

ب- فهرستی از بخش‌ها[4] و نقش‌های مسئول ساماندهی آسیب‌پذیری‌های بالقوه؛

پ- پادمان‌هایی[5] برای جلوگیری از افشای زود هنگام اطلاعات مربوط به آسیب‌پذیری‌های بالقوه قبل از

1- Internal-only
2- Basic guidance
3- Principles
4- Departments
5- Safeguards

این‌که آن‌ها مورد تعمیر قرار گیرند.
مخاطبین بخش عمومی خط‌مشی ساماندهی آسیب‌پذیری، ذی‌نفعان درونی و بیرونی هستند، ازجمله یابندگانی که خواهان گزارش دادن درباره آسیب‌پذیری‌های بالقوه هستند و کاربران محصولات یا خدمات برخط عرضه‌کننده. بخش عمومی مخاطبین را از این امر مطلع می‌کند که وقتی در محصولات یا خدمات برخط عرضه‌کننده یک آسیب‌پذیری بالقوه یافت می‌شود، عرضه‌کننده چگونه می‌خواهد با آن‌ها تعامل داشته باشد. رهنمودها، جزئیات و مثال‌های خط‌مشی‌های عمومی ساماندهی آسیب‌پذیری در بخش‌هایی از ISO/IEC 29147 که فرایندهای افشای آسیب‌پذیری را توصیف می‌کنند، شرح داده شده است.

۶-۳ توسعه چارچوب سازمانی برای حمایت از فرایندهای ساماندهی آسیب‌پذیری

۶-۳-۱ کلیات

ساماندهی آسیب‌پذیری‌ها جدای از مهندسی و فناوری، چندین جنبه اضافی دیگر نیز دارد (برای مثال، خدمات مشتریان و روابط عمومی). توصیه می‌شود یک چارچوب سازمانی، توسط بخش‌های ذی‌نفعان از عرضه‌کننده مسئول هر حوزه، طراحی، تشخیص داده و حمایت شود.
توصیه می‌شود سازمان، دارای نقش یا قابلیتی باشد که مسئولیت آن بر عهده آن سازمان بوده و دارای اختیار برای تصمیم‌گیری‌های مربوط به ساماندهی آسیب‌پذیری، ترجیحا در سطح مدیریتی باشد. این نقش یا قابلیت، باید از مسئولیت خویش در قبال کاربران عرضه‌کننده، فرایندهای درونی و چارچوب سازمانی برای ساماندهی آسیب‌پذیری آگاه باشد.
توصیه می‌شود سازمان، دارای یک نقش یا قابلیت به‌عنوان رابط کمیسیون برای ساماندهی آسیب‌پذیری‌های بالقوه باشد. توصیه می‌شود رابط کمیسیون برای هر بخش یا قسمت در عرضه‌کننده‌ای که محصولات یا خدمات برخط را در اختیار مشتریان قرار می‌دهد، مشخص شود.
توصیه می‌شود سازمان، برای طرف‌های بیرونی یک رابط کمیسیون تشکیل دهد تا بتواند در مورد آسیب‌پذیری‌ها به آنان دسترسی پیدا کرده و ارتباط برقرار کند. رابط کمیسیون ممکن است عضوی از یک گروه پاسخگویی به رخداد مربوط به امنیت رایانه (CSRIT عرضه‌کننده) یا یک گروه پاسخگویی به رخداد مربوط به امنیت محصول (PSRIT) باشد. جزئیات آن در ۶-۴ مورد بحث قرار گرفته‌اند.
از آنجا که مشتریان یا اصحاب رسانه ممکن است بعد از این‌که یک آسیب‌پذیری افشا شد، با سوالات یا درخواست‌هایی در مورد اطلاعات اضافی با عرضه‌کننده ارتباط برقرار کنند، بخش‌های مسئول مشتریان و روابط عمومی باید برای پاسخ‌گویی به این خواسته‌ها آماده باشند.

۶-۴ CSRIT یا PSRIT عرضه‌کننده

۶-۴-۱ کلیات

یک CSRIT یا PSRIT عرضه‌کننده مسئول هماهنگی گزارش‌های آسیب‌پذیری یابندگان بیرونی آسیب‌پذیری‌ها است. در بعضی موارد، یک PSRIT عرضه‌کننده آسیب‌پذیری‌هایی را که توسط گروه‌های

درونی عرضه‌کننده گزارش شده بودند را نیز هماهنگ می‌کند. عباراتی که در ادامه می‌آیند نقش سازمانی و مسئولیت‌های یک CSRIT یا PSRIT عرضه‌کننده را شرح می‌دهند. برای شفاف‌سازی، در ادامه استاندارد، برای ارجاع به این نقش از PSRIT استفاده خواهد شد.

۶-۴-۲ ماموریت گروه پاسخگویی به آسیب‌پذیری عرضه‌کننده

در فرایند ساماندهی آسیب‌پذیریِ عرضه‌کننده، PSRIT عرضه‌کننده نقش مرکزی را ایفا می‌کند. علاوه بر هماهنگی ساماندهی آسیب‌پذیری از درون، به‌عنوان تنها رابط کمیسیون برای ذی‌نفعان خارجی مانند یابندگان آسیب‌پذیری و هماهنگ‌کنندگان عمل می‌کند.
توصیه می‌شود عملکرد یک PSRIT عرضه‌کننده به‌طور متمرکز در درون عرضه‌کننده اجرایی شود، هرچند، در صورتی که تنها یک بخش تجاری وجود دارد که محصولات عمده و خدمات برخط عرضه‌کننده را ارائه می‌دهد، می‌تواند درون یک بخش تجاری محصولات نیز اجرایی شود.

۶-۴-۳ مسئولیت‌های گروه پاسخگویی به آسیب‌پذیری

۶-۴-۳-۱ کلیات

این بند، مسئولیت‌های گروه‌های پاسخگویی به آسیب‌پذیری را شرح می‌دهد.

۶-۴-۳-۲ ارتباط با یابندگان بیرونی آسیب‌پذیری‌های بالقوه

توصیه می‌شود یک PSRIT عرضه‌کننده، نقطه‌ی ورودی واحد برای دریافت گزارش‌های آسیب‌پذیری بالقوه از یابندگان یا هماهنگ‌کنندگان تشکیل دهد، که معمولا به‌صورت یک آدرس رایانامه یا یک فرم بر روی یک صفحه وب است.
یک PSRIT عرضه‌کننده مسئول حفظ ارتباط با یابندگانی است که آسیب‌پذیری‌های بالقوه را گزارش کرده-اند. برای عرضه‌کنندگان مهم است که اهمیت سروقت بودن و دستور کارها و مواضع متفاوت یابندگان در قبال آسیب‌پذیری‌ها را درک کنند.

۶-۴-۳-۳ ارتباط با بخش‌های تجاری محصولات

یک PSRIT عرضه‌کننده باید جهت ایجاد پایگاه داده‌های رابطین هر محصول، با بخش‌های محصولات و خدمات برخط عمل کند. وقتی‌که یک آسیب‌پذیری بالقوه گزارش می‌شود، PSRIT باید مسئول بخش تجاری محصول را تشخیص دهد تا از طریق شخص رابط، گزارش را برای آنان ارسال کند. اطلاعات باید به‌صورت محرمانه و بر پایه میزان نیاز به دانستن آن‌ها، به اشتراک گذاشته شوند.

۶-۴-۳-۴ ارتباط با هماهنگ‌کننده‌ها یا عرضه‌کنندگان دیگر

یک PSRIT عرضه‌کننده باید در مواقع مناسب، تمهیدی برای به اشتراک‌گذاری اطلاعات آسیب‌پذیری با

هماهنگ‌کننده‌ها یا عرضه‌کنندگان دیگر ترتیب دهد. توصیه می‌شود آن‌ها از خط‌مشی ساماندهی آسیب‌پذیری طرف دیگر آگاه باشند.

۶-۴-۳-۵ زمان‌بندی افشای آسیب‌پذیری

یک PSRIT عرضه‌کننده باید تاریخ مناسبی برای افشای هرکدام از آسیب‌پذیری‌ها انتخاب کرده و به کمک بخش تجاری محصول و ذی‌نفعان مهم دیگر مانند هماهنگ‌کننده‌ها، در صورت امکان مشاوره‌هایی را ارائه کند.

۶-۴-۳-۶ پایش آسیب‌پذیری عمومی

توصیه می‌شود PSRIT عرضه‌کننده منابع عمومی شناخته شده اطلاعات آسیب‌پذیری را جهت افشا یا بحث در مورد چیزهایی که بر محصولات یا خدمات برخط عرضه‌کننده تاثیر می‌گذارند مورد پایش قرار دهد. این امر ممکن است شامل نظرآزمایی‌های متن‌باز[1] یا دادگان‌های آسیب‌پذیری باشد.

۶-۴-۴ قابلیت‌های کارکنان

توصیه می‌شود کارکنان PSRIT عرضه‌کننده:

الف- قادر به فهم ماهیت آسیب‌پذیری‌های بالقوه گزارش شده بوده و آن‌ها را به طرف‌های مرتبط ارسال کنند؛

ب- محرمانگی اطلاعات مرتبط با آسیب‌پذیری را درک کرده و به‌خوبی دانش ساماندهی چنین اطلاعاتی را داشته باشند تا قبل از تدوین راه‌حل جزئیات آسیب‌پذیری را افشا نکنند؛

پ- بخش تجاری محصول مناسب را در زمان مناسب، آگاه سازند تا اقدامات لازم برای ساماندهی آسیب‌پذیری را انجام کنند.

۶-۵ مسئولیت‌های بخش تجاری محصول

بخش تجاری محصول، محصولات یا خدمات برخطی را که توسط عرضه‌کننده توسعه یافته‌اند یا توسط محصولات یا خدمات برخط دیگر عرضه‌کننده پیاده‌سازی و/یا تبلیغ شده‌اند را در اختیار مشتریان قرار می‌دهد. هر یک آن‌ها هستار[2] هستند که مسئول یک بخش مرکزی فرایند ساماندهی آسیب‌پذیری‌هایی است که محصولات یا خدمات برخط آن‌ها را تحت تاثیر قرار می‌دهند.

وقتی‌که آسیب‌پذیری‌های بالقوه توسط PSRIT عرضه‌کننده به یک بخش تجاری محصول گزارش می‌شوند، باید بخش تجاری محصول با PSRIT کار کند تا اقدامات ترمیم را توسعه دهند. اگر مشخص شود که یک موضوع، در واقع یک آسیب‌پذیری است و نه یک نوع متفاوت از اشکال[3]، توصیه می‌شود بخش تجاری ابزاری

1- Open source forums
2- Entity
3- Bug

برای رساندن یک موضوع به PSRIT داشته باشد.
رابطین امنیت محصول در داخل بخش‌های تجاری، توصیه می‌شود وقتی‌که هشدارهایی در مورد آسیب‌پذیری‌های بالقوه امنیتی در محصولات یا خدمات برخط دریافت می‌کنند، فرایند ساماندهی آسیب‌پذیری را آغاز کنند. توصیه می‌شود این فرایند شامل هشداردهی به PSRIT باشد تا هر اقدام ضروری در جهت پاسخ‌گویی، متناظر با خط‌مشی‌های رویارویی با آسیب‌پذیری‌های عرضه‌کننده، اجرایی شود.

۶-۶ مسئولیت‌های بخش حمایت از مشتری و بخش روابط عمومی

در مراحل نهایی ساماندهی آسیب‌پذیری، مشاوره‌ها اغلب به همراه ترمیم‌ها عرضه می‌گردند. وقتی‌که مشاوره‌ها از طریق فهرست‌های پستی و یا تماس مستقیم به مشتریان فرستاده می‌شوند، پراکنش[1] اغلب توسط بخش‌های پشتیبانی از مشتری هدایت می‌شود. توصیه می‌شود پشتیبانی از مشتری وسیله مناسب برای اطلاع‌رسانی به همه مشتریان ضروری را انتخاب کرده و تا تاریخ هماهنگ شده برای افشا، محرمانگی را حفظ کند. برای زمان‌بندی انتشار مشاوره در آسیب‌پذیری‌های چند-عرضه‌کننده[2] به استاندارد ISO/IEC 29147 مراجعه شود.
ممکن است بعضی از مشتریان پس از مطالعه مشاوره، سوالاتی بپرسند یا خواستار پشتیبانی عرضه‌کننده شوند. توصیه می‌شود بخش‌های پشتیبانی از مشتری آمادگی پاسخگویی یا حل سوالات و درخواست‌های مرتبط با مشاوره باشند.
همان‌طور که در استاندارد ISO/IEC 29147 با جزئیات آمده است، مشاوره‌هایی که بر روی وبگاه عمومی یک عرضه‌کننده منتشر شده‌اند، توصیه می‌شود به‌راحتی قابل دسترس باشند. بخش‌های پشتیبانی از مشتری یا روابط عمومی ممکن است در نگهداری از وبگاه عرضه‌کننده دخیل باشند و توصیه می‌شود تلاش کنند تا به رهنمودهای ISO/IEC 29147 پایبند باشند.
اگر یک آسیب‌پذیری افشاشده موضوعی جدی یا فراگیر است، توصیه می‌شود بخش‌های روابط عمومی آماده تماس از طرف رسانه‌های جمعی باشند.

۷-۶ مشاوره حقوقی

عرضه‌کنندگان ممکن است نیاز به بازبینی حقوقی ترمیم‌های ارائه شده و ارتباطات داشته باشند تا اطمینان حاصل کنند که از خط‌مشی‌های درونی، قوانین، و معاهده‌های موجود تبعیت می‌کنند.

1- Dissemination
2- Multi-vendor

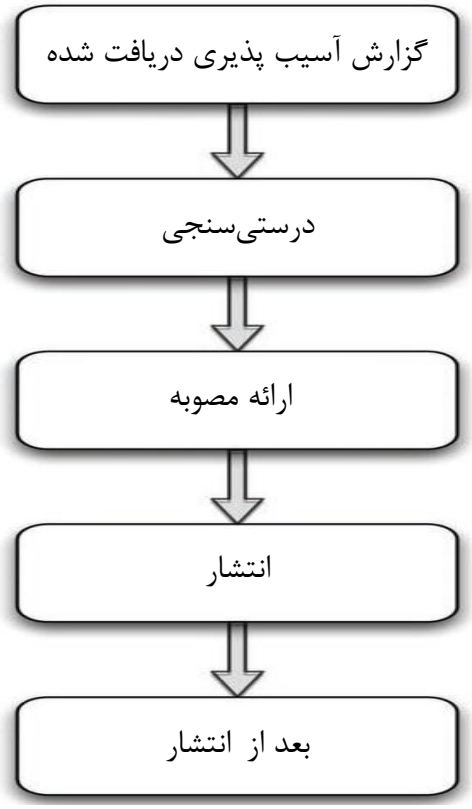
۷ فرایند ساماندهی آسیب‌پذیری

۷-۱ معرفی مراحل ساماندهی آسیب‌پذیری

شکل ۲ یک فرایند نوعی ساماندهی آسیب‌پذیری را نشان می‌دهد. چنین فرایندی معمولا توسط عرضه‌کننده اجرا می‌شود.

توصیه می‌شود، فرایند ساماندهی آسیب‌پذیری ملزم باشند که توصیفی از طبیعت و تاثیرات هرکدام از نواقص امنیتی و وضعیت پیدا کردن تصحیحی برای آن نقص، ثبت گردد.

یکی از اهداف یک فرایند ساماندهی آسیب‌پذیری تدارک یک راه‌حل به‌موقع برای آسیب‌پذیری‌های بالقوه است.



شکل ۲- یک مدل از ساماندهی آسیب‌پذیری

۷-۲ مراحل ساماندهی آسیب‌پذیری

۷-۲-۱ کلیات

این زیربند مراحل معمول که هنگام پردازش گزارش‌های آسیب‌پذیری رخ می‌دهند را توصیف می‌کند. این زیربند نقطه شروعی را برای عرضه‌کننده فراهم می‌کند تا فرایندهای مرتبط را درک کند و به او امکان می‌دهد فرایندهای درونی را ایجاد کند یا تغییر دهد تا در هر موقعیت، به هنگام بروز آن بتوان برخورد مناسب را انجام داد.

۷-۲-۲ گزارش آسیب‌پذیری دریافت شده

این زیربند عرضه‌کننده‌ای را توصیف می‌کند که از منابع درونی یا بیرونی یک گزارش آسیب‌پذیری را دریافت می‌کند. ممکن است دو منبع در نظر گرفته شوند:

الف- **آسیب‌پذیری‌هایی که از درون یافت شده‌اند و آسیب‌پذیری‌هایی بالقوه**: یک آسیب‌پذیری که حین توسعه چرخه زندگی یا بعد از انتشار محصول توسط عرضه‌کننده کشف شده است.

ب- **آسیب‌پذیری‌هایی که از بیرون یافت شده‌اند و آسیب‌پذیری‌های بالقوه**: یک آسیب‌پذیری که توسط فرد یا سازمانی خارج از عرضه‌کننده کشف شده است. برای واسط با منابع آسیب‌پذیری‌های خارجی به استاندارد ISO/IEC 29147 مراجعه شود.

۷-۲-۳ درستی‌سنجی[1]

این زیربند درستی‌سنجی در تمام انواع آسیب‌پذیری‌های دریافت شده را توصیف می‌کند. توصیه می‌شود تمامی سوابق آسیب‌پذیری‌ها و آسیب‌پذیری‌های بالقوه‌ی دریافت شده و پردازش شده توسط عرضه‌کننده از هر منبعی ثبت شوند. در طول درستی‌سنجی، فعالیت‌هایی که در ادامه می‌آیند رخ خواهند داد. همان‌گونه که در زیر شرح داده شده است، برخی از فرایندهای ذیل ممکن است به‌جای سلسله‌وار بودن، به‌صورت موازی رخ دهند.

الف- **بررسی اولیه**: اگر مشکلی در رابطه با یک محصول یا خدمت برخطی که تحت پشتیبانی عرضه-کننده است رخ دهد، عرضه‌کننده سعی می‌کند که آسیب‌پذیری بالقوه را تایید کند. حتی اگر آسیب‌پذیری بالقوه در نرم‌افزار یا خدمتی پیدا شود که در حال حاضر پشتیبانی نمی‌شود، توصیه می‌شود بررسی ادامه پیدا کند تا مشخص شود که آیا مشکل بر محصولات یا خدمات پشتیبانی شده نیز تاثیر می‌گذارد یا نه. عرضه-کننده شدت آسیب‌پذیری گزارش شده را تعیین می‌کند.

ب- **خروج احتمالی از فرایند**: اگر آسیب‌پذیری بالقوه قادر به تایید شدن یا بازتولید نباشد یا عرضه-کننده تایید کند که آن مشکل یک آسیب‌پذیری امنیتی محسوب نمی‌شود، عرضه‌کننده از فرایند ساماندهی آسیب‌پذیری خارج خواهد شد. اگر آسیب‌پذیری بالقوه توسط فرد یا سازمانی بیرون از عرضه‌کننده کشف و گزارش شده باشد، آن‌گاه همچنین به استاندارد ISO/IEC 29147 مراجعه شود که توصیه‌هایی را شرح می‌دهد که عرضه‌کننده از هستار بیرونی سوالات بیشتری را پرسش کند تا تلاش کند که قبل از بسته شدن بررسی موضوع را با موفقیت بازتولید کند.

شرایط دیگر نیز ممکن است باعث شوند که عرضه‌کننده در مورد مشکل مشخص تحت بررسی از فرایند ساماندهی آسیب‌پذیری خارج شود. اگر آسیب‌پذیری بالقوه توسط فرد یا سازمانی بیرون از عرضه‌کننده گزارش شده باشد، آن‌گاه همچنین به استاندارد ISO/IEC 29147 مراجعه شود تا دلیل خروج از فرایند را به اطلاع یابنده مشکل برسانید، ازجمله:

1- Verification

۱- **اشکال تکراری**: مشکل یک آسیب‌پذیری است که قبلا نیز تکرار شده است و در حال حاضر تحت فرایند قرار دارد و یا توسط عرضه‌کننده رفع شده است.

۲- **اشکال مربوط به محصول منسوخ‌شده**: آسیب‌پذیری در محصولی است که دیگر توسط عرضه‌کننده پشتیبانی نمی‌شود.

۳- **اشکال غیرامنیتی**: این اشکال هیچ‌گونه تاثیر امنیتی نداشته و یا با فنون شناخته شده در حال حاضر نمی‌تواند مورد بهره‌جویی قرار گیرد. توصیه می‌شود، عرضه‌کننده‌ها توجه داشته باشند که بهره‌جویی‌ها از یک اشکال می‌توانند با فنون جدید یا بردارهای حمله تغییر کنند، بنابراین توصیه می‌شود عرضه‌کننده‌ها سعی کنند از فنون بهره‌جویی آگاه باشند. این اشکالات می‌توانند توسط فرایند منظم رفع اشکالات عرضه‌کننده برطرف گردند.

۴- **اشکال طرف سوم**: آسیب‌پذیری به علت کد یا پیکربندی طرف سوم بوده و یا در یک حالت خاصی وجود دارد که عرضه‌کننده به‌طور مستقیم مسئول آن نیست. توصیه می‌شود، از طریق روش‌های شرح داده شده در استاندارد ISO/IEC 29147 مشکل در اختیار طرف‌هایی قرار گیرد که مسئول هستند.

پ- **تحلیل علت ریشه‌ای**: عرضه‌کننده سعی می‌کند که علل اصلی آسیب‌پذیری را تعیین کرده و سعی می‌کند محصولات تاثیر پذیرفته را تشخیص دهد، ازجمله تمامی روش‌های احتمالی بهره‌جویی، زیرا آن‌ها با آسیب‌پذیری ارتباط دارند.

ت- **بررسی بیشتر**: عرضه‌کننده تلاش می‌کند تا مثال‌های دیگری از همان نوع آسیب‌پذیری را در محصولات یا خدمات دیگر عرضه‌کننده پیدا کند. بررسی می‌تواند به نسخه‌های قبلی یا بعدی محصول یا خدمت نیز توسعه پیدا کرده و ممکن است شامل محصولات یا خدمات دیگر عرضه‌کننده نیز شود.

ث- **اولویت‌بندی**: عرضه‌کننده تهدید ایجادشده توسط آسیب‌پذیری برای کاربران تاثیر پذیرفته محصول یا خدمت برخط را در نظر می‌گیرد. برای هر محصول یا خدمت تاثیر پذیرفته ممکن است شدت‌های مختلفی برای همان مشکل وجود داشته باشد. هر وقت که ممکن باشد، توصیه می‌شود عرضه‌کننده شدت یک آسیب‌پذیری را در شرایطی از محصول یا خدمت که بیش از همه به کار گرفته می‌شود تعیین کند تا به اولویت‌بندی کمک کند. عرضه‌کنندگان ممکن است در تعیین فوریت نسبی ارائه یک راه‌حل عوامل مختلفی را در نظر بگیرند، مانند تاثیر بالقوه، احتمال بهره‌جویی، و محدوده کاربران تاثیر پذیرنده.

۷-۲-۴ ارائه راه‌حل

این زیربند توسعه راه‌حل برای آسیب‌پذیری را توصیف می‌کند. توصیه می‌شود گام‌های ذیل در ترتیب سلسله‌وار رخ دهند.

الف- **تصمیم برای راه‌حل**: عرضه‌کننده تعیین می‌کند که چگونه آسیب‌پذیری می‌تواند به‌صورت جامع حل شود، چگونه تاثیر بهره‌جویی موفق از آسیب‌پذیری را کاهش داد، یا چگونه قرارگیری در معرض خطر را کاهش داد.

هنگام تعیین بهترین راه‌حل، توصیه می‌شود عرضه‌کننده سعی کند نیاز به ایجاد سریع یک راه‌حل را با

آزمون‌های ضروری کلی مورد در تعادل قرار دهد تا مطمئن شود که راه‌حل، به علت مشکلات کیفی، تاثیر منفی بر روی کاربران تحت تاثیر نمی‌گذارد. برای تعیین این راه‌حل، توصیه می‌شود عرضه‌کننده چند عامل را در نظر بگیرد، مثل این‌که آیا یک آسیب‌پذیری، به علت این‌که بهره‌جویی از آن آسان است یا این‌که مشکل در حال حاضر به‌صورت فعال مورد بهره‌جویی قرار می‌گیرد، مخاطره بالایی برای بهره‌جویی از کاربران تاثیرپذیر را در بر دارد یا نه. در مواردی که یک آسیب‌پذیری مخاطره بالایی را برای کاربران در بر دارد، یک راه‌حل موقتی یا میان مدت که شامل کاهش خطرات است، ممکن است مورد نیاز باشد. در شرایط دارای مخاطره بالا، یک راه‌حل غیر جامع که در اغلب فرانامه‌ها[1] کار می‌کند ممکن است ضروری باشد.

ب- **ایجاد ترمیم**: عرضه‌کننده، وصله(ها)، تعمیر(ات)، ارتقا(ها)، یا مستندسازی یا تغییر(ات) پیکربندی را برای مقابله با یک آسیب‌پذیری ایجاد می‌کند. این گام همچنین ممکن است شامل تصمیم جهت اطلاع‌رسانی به یک مجری ثانوی قرارداد یا مسئول شبکه عرضه‌کننده باشد تا صفحه یا صفحات آسیب‌پذیر را برون‌خط[2] کنند یا ممکن است شامل اطلاع‌رسانی به یک شرکت انتشاری باشد برای لغو برنامه آسیب‌پذیری عرضه‌کننده.

پ- **امتحان ترمیم**: عرضه‌کننده آزمون‌های مناسبی را توسعه داده و انجام می‌دهد تا مطمئن شود که به مشکل مربوط به آسیب‌پذیری، در تمام چارچوب‌های تحت پشتیبانی، پاسخگویی شده است. توصیه می‌شود عرضه‌کننده تلاش کند که اطمینان حاصل کند که ترمیم باعث بروز آسیب‌پذیری‌های جدید یا مشکلات کلی مربوط به کیفیت محصول نشده و یا با محصولات یا خدمات دیگر از نظر سازگاری مشکلی ندارد. اگر در طول آزمون ترمیم با شکست مواجه شود، عرضه‌کننده ممکن است ترمیم را تغییر داده یا ترمیم‌های جدیدی را تولید کرده و گام‌های قبلی فرایند را تکرار کند.

۷-۲-۵ ارائه راه‌حل آسیب‌پذیری به گام بعدی فرایند

این زیربند انتشار راه‌حل یک آسیب‌پذیری را شرح می‌دهد. اگر آسیب‌پذیری توسط یک هستار بیرونی گزارش شده باشد، آن‌گاه برای واسط با طرف‌های مرتبط بیرونی به استاندارد ISO/IEC 29147 مراجعه شود. فهرستی که در ادامه می‌آید، دو راه متفاوت که یک عرضه‌کننده به منظور حل آسیب‌پذیری می‌تواند طی کند را شرح می‌دهد. به‌طور معمول فقط یکی از راه‌ها طی می‌شود، اما مواردی هم وجود دارند که برای رسیدگی به یک آسیب‌پذیری به مولفه‌هایی از هر دو فرانامه نیاز داریم. برای مثال، عرضه‌کننده‌ای که در خدمات برخط خود بر روی سامانه‌های خود تغییری ایجاد می‌کند، ممکن است نیاز داشته باشد که از کاربران خود بخواهد که جهت رفع کامل آسیب‌پذیری رمز عبور خود را تغییر داده و یا از سامانه خارج شده و دوباره به آن وارد شوند. ارتباط با کاربران جهت راهنمایی آن‌ها برای عمل کردن، از طریق استاندارد ISO/IEC 29147 و در یک مشاوره ایمنی که توسط عرضه‌کننده ارائه می‌شود، ساماندهی خواهد شد.

الف- **راه‌حل برای آسیب‌پذیری خدمات برخط**: برای آسیب‌پذیری‌های خدمات برخط، توصیه می‌شود

1- Scenarios
2- Off-line

عرضه‌کنندگان از فرایندهای ارتقا دادن یا تغییرات پیکربندی سازمان خودشان برای سامانه‌های تولید استفاده کنند.

ب- **راه‌حل برای آسیب‌پذیری محصول**: به‌محض این‌که عرضه‌کننده از اثربخشی ترمیم احساس رضایت کرد، ترمیم را از طریق فرایندهای تعریف شده در استاندارد ISO/IEC 29147 انتشار خواهد داد.

۷-۲-۶ فعالیت‌های مربوط به بعد از راه‌حل

این زیربند فعالیت‌های عرضه‌کننده بعد از انتشار راه‌حل آسیب‌پذیری را شرح می‌دهد. عناصر این فهرست می‌توانند به‌صورت موازی انجام شوند.

الف- **نگهداری مورد**: پس از این‌که راه‌حل منتشر شد، به‌روزرسانی‌های بیشتری ممکن است برای راه‌حل صورت پذیرد. عرضه‌کننده راه‌حل‌ها را به‌صورت مناسب به‌روزرسانی می‌کند، معمولا تا وقتی‌که به‌روزرسانی‌های بیشتر دیگر محل بحث نباشند، مراحل قبلی فرایند ساماندهی آسیب‌پذیری مانند مرحله درستی‌سنجی یا مرحله توسعه راه‌حل را تکرار می‌کند.

ب- **بازخورد چرخه زندگی توسعه امنیت**: عرضه‌کننده با استفاده از اطلاعات به دست آمده در طول فرایند نوشتن راه‌حل و در طول تحلیل علت ریشه‌ای، چرخه توسعه را به‌روزرسانی می‌کند تا از آسیب‌پذیری‌های مشابه در محصولات یا خدمات جدید یا به‌روزرسانی شده جلوگیری کند. به استاندارد ISO/IEC 27034 مراجعه شود.

پ- **پایش**: در مورد مربوط به رفع آسیب‌پذیری‌های خدمات برخط، بعد از این‌که عرضه‌کننده از ترمیم استفاده می‌کند، توصیه می‌شود عرضه‌کننده ثبات محصول یا خدمت را پایش کند.

۷-۳ پایش مراحل ساماندهی آسیب‌پذیری

توصیه می‌شود عرضه‌کنندگان اثربخشی فرایندهای ساماندهی آسیب‌پذیری‌شان را پایش کنند. این زیربند جنبه‌هایی از فرایند ساماندهی آسیب‌پذیری که توصیه می‌شود مورد پایش قرار گیرند را شرح می‌دهد.

الف- **سرعت**: توصیه می‌شود عرضه‌کنندگان زمانی که طول می‌کشد تا با استفاده از این فرایند به یک آسیب‌پذیری پرداخته شود را مورد پایش قرار دهند و سعی کنند سرعت رفع آسیب‌پذیری را ارتقا بخشند. در مواردی که سطح مخاطره آسیب‌پذیری بالا است، رفع سریع آسیب‌پذیری می‌تواند کمک کند تا از انتشار خسارات جلوگیری کرد.

ب- **کامل بودن**: توصیه می‌شود عرضه‌کنندگان کامل بودن ترمیم را مورد پایش قرار دهند تا مطمئن باشند که این راه‌حل به علت ریشه‌ای آسیب‌پذیری می‌پردازد. تحلیل علت ریشه‌ای که در مرحله درستی‌سنجی فرایند ساماندهی آسیب‌پذیری انجام می‌شود، برای کامل بودن ترمیم بسیار حیاتی است. هرچند، اگر برای رفع یک آسیب‌پذیری که هم‌اکنون مورد بهره‌جویی قرار گرفته فوریت وجود دارد، عرضه-کنندگان می‌توانند ترمیم ناکامل را به‌عنوان راه‌حل موقتی ایجاد کنند، به هر جهت وقتی این جنبه از فرایندهای ساماندهی آسیب‌پذیری را مورد پایش قرار می‌دهیم، توصیه می‌شود این موضوع را هم مدنظر

داشته باشیم.

پ- **تداوم**: توصیه می‌شود عرضه‌کنندگان پس از این‌که راه‌حل در اختیار کاربران تاثیر پذیرفته قرار گرفت، اثربخشی آن را مورد پایش قرار دهد. عرضه‌کننده باید توجه کند که راه‌حل ارائه شده چه مدت حفظ می‌شود تا اثربخشی راه‌حل آسیب‌پذیری را ارزیابی کند.

۴-۷ محرمانگی اطلاعات آسیب‌پذیری

توصیه می‌شود عرضه‌کنندگان مراقب باشند که محرمانگی اطلاعات حساس آسیب‌پذیری حفظ شود. دو رده مهم از اطلاعات وجود دارند که باید حفظ شوند. رده اول اطلاعات شخصی یا مربوط به هستار سازمان است، مانند نام یابنده‌ای که سعی دارد ناشناس بماند، یا آدرس قرارداد اینترنتی (IP)[1] مشتری که به علت بهره-جویی از یک آسیب‌پذیری آسیب‌دیده است. رده دوم آن دسته از اطلاعات آسیب‌پذیری است که هنوز انتشار نیافته و یا همگانی نشده است، مانند یک آسیب‌پذیری که هنوز تحت بررسی بوده یا جزئیات فنی که بیش از حد به مهاجمین سود می‌رسانند.

توصیه می‌شود عرضه‌کنندگان از شیوه‌های معقول عملیاتی امنیتی پیروی کنند تا از اطلاعات آسیب‌پذیری محافظت کنند. این فعالیت‌ها ممکن است شامل محدود کردن دسترسی واحدهای سازمانی یا کارکنان بر اساس میزان نیاز به دانستن و رمزگذاری داده‌ها برای انتقال از طریق کانال‌های غیرمطمئنی مثل رایانامه باشد.

افشای زود هنگام اطلاعات آسیب‌پذیری حساس می‌تواند مخاطرات و هزینه‌های مربوط به افشای اطلاعات را برای عرضه‌کننده و کاربران بالا ببرد. توصیه می‌شود سطح محرمانگی بر این اساس باشد که چه اطلاعاتی می‌توانند مورد بهره‌جویی قرار گیرند و کدام اطلاعات هم‌اکنون به‌صورت عمومی در دسترس هستند.

۸ فرایند ساماندهی آسیب‌پذیری زنجیره تامین

این بند، فرایندهای ساماندهی آسیب‌پذیری را درزمانی توضیح می‌دهد که آسیب‌پذیری، مولفه‌هایی را که توسط محصولات طرف‌های دیگر مورد استفاده قرار می‌گیرند تحت تاثیر قرار می‌دهد.

یکی از عواملی که عرضه‌کنندگان باید به‌عنوان بخشی از تصمیم‌گیری راه‌حل خود مدنظر قرار دهند وابستگی محصولات و خدمات برخط به محصولات و خدمات برخط خود عرضه‌کننده یا عرضه‌کنندگان دیگر است. اگر یک محصول یا خدمت تاثیر پذیرفته بخشی از زنجیره تامین یک عرضه‌کننده دیگر است، توصیه می‌شود عرضه‌کننده، اگر ممکن است، سعی کند عرضه‌کنندگان تاثیر پذیرفته دیگر را در بحث در مورد مصوبات بالقوه سهیم کند.

موارد دیگری که عرضه‌کنندگان ممکن است اطلاعات آسیب‌پذیری را برای حل مشکلی که شامل اجزایی از عرضه‌کنندگان متعدد است به اشتراک بگذارد، شامل این موارد است:

1- Internet Protocol

الف- یک آسیب‌پذیری گزارش شده که یک نوع خاص نرم‌افزار را تحت تاثیر قرار می‌دهد اما به علت مشکل در یک سامانه عامل مشخص یا CPU به وجود آمده است؛

ب- آسیب‌پذیری‌ها در اجرای محصولات مختلفی که بر اساس یک استاندارد معیوب یا الگوریتم‌های انتشار یافته ساخته شده‌اند؛

پ- آسیب‌پذیری‌هایی که به علت روشگان[1] توسعه مورد قبول عام به وجود آمده‌اند؛

ت- آسیب‌پذیری‌ها در کتابخانه‌هایی که به‌طور عام مورد استفاده قرار می‌گیرند؛

ث- آسیب‌پذیری‌ها در مولفه‌های نرم‌افزاری که در حال حاضر فاقد یک نگاه‌دار فعلی هستند.

به استاندارد ISO/IEC 28001 مراجعه شود[۴].

1- Methodology

کتاب‌نامه

[۱] استاندارد ملی ایران شماره ۳-۱۵۴۰۸: سال ۱۳۹۰، فناوری اطلاعات -فنون امنیتی -معیار ارزیابی امنیت فناوری اطلاعات -قسمت ۳- مولفه‌های تضمین امنیتی

[۲] استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سامانه‌های مدیریت امنیت اطلاعات – الزامات

[3] ISO/IEC 27034, Information technology – Security techniques - Application security

[4] ISO 28001, Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance

[5] ISO/IEC 29147, Information technology — Security techniques — Vulnerability disclosure