INSO

19055

1st. Edition

2015

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

استاندارد ملی ایران
۱۹۰۵۵
چاپ اول
۱۳۹۳

فناوری اطلاعات – فنون امنیتی- افشای آسیب‌پذیری

Information technology — Security Techniques — Vulnerability disclosure

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی 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 می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (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 of Legal Metrology (Organisation Internationale de Metrologie Legale)

4 - Contact point

5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات – فنون امنیتی- افشای آسیب‌پذیری»

رئیس:	**سمت و/یا نمایندگی**
معروف، سینا (لیسانس مهندسی کامپیوتر، سخت‌افزار)	کارشناس سازمان فناوری اطلاعات ایران
دبیر:	
یزدیان ورجانی، علی (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس و مسئول مرکز آپا دانشگاه تربیت مدرس

اعضا: (اسامی به ترتیب حروف الفبا)

اسدی‌پویا، سمیرا (فوق لیسانس مهندسی فناوری اطلاعات)	مدیر عامل شرکت مهندسی پویا دانش و کیفیت آوا
ایزدپناه، سحر سادات (فوق لیسانس مهندسی فناوری اطلاعات)	رییس اداره تدوین استاندارد سازمان فناوری اطلاعات ایران
شیرازی، مریم (لیسانس فناوری اطلاعات)	کارشناس پژوهشگاه استاندارد سازمان ملی استاندارد ایران
شیخ‌الاسلامی، محمد کاظم (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس
صادقی، مریم (لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس سازمان نظام صنفی رایانه‌ای کشور
طی‌نیا، رضا (فوق لیسانس مهندسی فناوری اطلاعات)	مدیرعامل شرکت مهندسی کاربرد سیستم
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس حقیقی تدوین استاندارد سازمان ملی استاندارد ایران

قسمتی، سیمین (فوق لیسانس مهندسی فناوری اطلاعات)	مشاور مرکز آپا دانشگاه تربیت مدرس
قندهاری، آزاده (فوق لیسانس هوش مصنوعی)	کارشناس مرکز تحقیقات مخابرات ایران
محمدیان، مصطفی (دکتری، برق)	عضو هیات علمی و معاون پژوهشی دانشکده برق و کامپیوتر دانشگاه تربیت مدرس

فهرست مندرجات

پیشگفتار

استاندارد «فناوری اطلاعات – فنون امنیتی- افشای آسیب‌پذیری» که پیش‌نویس آن در کمیسیون‌های مربوط توسط مرکز آپا (آگاهی‌رسانی، امداد، پشتیبانی رخدادهای رایانه‌ای) دانشگاه تربیت مدرس تهیه و تدوین شده است و در سیصد و پنجاه و پنجمین اجلاس کمیته ملی استاندارد فناوری اطلاعات مورخ ۹۳/۱۰/۲۷ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

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

ISO/IEC 29147:2014, Information technology — Security techniques — Vulnerability disclosure

فناوری اطلاعات – فنون امنیتی- افشای آسیب‌پذیری

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین خطوط راهنما برای افشای آسیب‌پذیری‌های بالقوه در محصولات و خدمات برخط[1] است. این استاندارد ملی جزئیات روش‌هایی را ارائه می‌کند که عرضه‌کننده[2] از آن برای پرداختن به مسائل مربوط به افشای آسیب‌پذیری استفاده می‌کند. این استاندارد ملی:

الف) خطوط راهنمایی را به عرضه‌کنندگان در مورد چگونگی دریافت اطلاعات در مورد آسیب‌پذیری‌های بالقوه در محصولات یا خدمات برخط، ارائه می‌کند.

ب) خطوط راهنمایی را به عرضه‌کنندگان در مورد چگونگی انتشار اطلاعات رفع[3] آسیب‌پذیری‌ها در محصولات یا خدمات برخط ارائه می‌کند.

پ) اقلام اطلاعاتی که باید در پیاده‌سازی فرآیند افشای آسیب‌پذیری عرضه‌کننده تولید شود را ارائه می‌کند.

و

ت) مثال‌هایی از محتوایی که باید در اقلام اطلاعاتی گنجانده شود را ارائه می‌کند.

این استاندارد ملی برای عرضه‌کنندگانی کاربردپذیر است که به گزارش‌های بیرونی آسیب‌پذیری‌ها در محصولات یا خدمات برخط خود پاسخ می‌دهند.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آنها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آنها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آنها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 27000:2012, *Information technology — Security techniques — Information security management*

2-2 ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*

---

1 - Online
2 - Vendor
3 - Resolution

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌رود:

۳-۱ توصیه

اطلاعیه یا خبرنامه‌ای که جهت اطلاع‌رسانی به کار گرفته می‌شود و در مورد آسیب‌پذیری یک محصول هشدار می‌دهد.

یادآوری ۱ – توصیه ممکن است شامل نصیحتی در مورد چگونگی مقابله با آسیب‌پذیری باشد. توصیه به صورت نمونه شامل توصیفی از آسیب‌پذیری در یک زمان خاص است. توصیه می‌تواند شامل فهرست محصولات یا خدمات آسیب‌پذیر، اثر بالقوه، اطلاعات رفع و کاهش آسیب‌پذیری و مراجع باشد. اقلام موجود در توصیه به زمان انتشار توصیه بستگی دارد و ممکن است با گذشت زمان تغییر کند. توصیه ممکن است توسط عرضه‌کننده، یابنده، یا هماهنگ‌کننده منتشر شود و ممکن است با در دست داشتن اطلاعات بیشتر ویرایش شود.

۳-۲ هماهنگ‌کننده

شرکت‌کننده اختیاری که می‌تواند به عرضه‌کنندگان و یابندگان[1] در ساماندهی و افشای اطلاعات آسیب‌پذیری کمک کند.

یادآروی ۱ - هماهنگ‌کننده می‌تواند با ایجاد ارتباط مثبت بین طرف‌های معامله (عرضه‌کنندگان و یابندگان) به عنوان رابط مورد اعتماد بین آن‌ها عمل کند.

۳-۳ یابنده

فرد یا سازمانی که آسیب‌پذیری بالقوه‌ای را در محصول یا خدمت[2] برخط شناسایی می‌کند.

یادآوری ۱– یابندگان می‌توانند محققین، شرکت‌های امنیتی، کاربران، دولت‌ها، یا هماهنگ‌کننده‌ها باشند.

۳-۴ خدمات برخط

خدمتی که توسط سخت‌افزار، نرم‌افزار یا ترکیبی از هر دو پیاده‌سازی می‌شود و روی یک خط ارتباطی یا شبکه ارائه می‌شود.

یادآوری ۱ – خدمات برخط مشابه محصولات بوده و هر دو در واقع یک سامانه نرم افزاری هستند. دو وجه تمایز مهم این است که اغلب خدمت برای کاربران به عنوان نمونه منفرد نرم‌افزاری ظاهر می‌شود و کاربران نرم‌افزار را نصب، مدیریت، یا جایگزین نمی‌کنند و آنها فقط از خدمت استفاده می‌کنند.

۳-۵ محصول

سامانه‌ای که برای فروش پیاده‌سازی توسعه داده می‌شود یا به صورت رایگان ارائه می‌شود.

۳-۶ بازسازی[3]

وصله[4]، اصلاحیه[1]، ارتقا، پیکربندی یا تغییر مستندات برای حذف یا کاهش آسیب‌پذیری است.

---

1 - Finders
2 - Service
3 - Remediation
4 - Patch

یادآوری ۱ – بازسازی به طور معمول شکل تغییر پیکربندی، جایگزینی پرونده دودویی، تغییر سخت‌افزاری، وصله کد منبع و غیره را در بر می‌گیرد. بازسازی به طور معمول توسط عرضه‌کنندگان ارائه می‌شود. عرضه‌کنندگان از اصطلاحات متفاوتی شامل وصله، اصلاحیه، هات فیکس[2] و ارتقا استفاده می‌کنند.

یادآوری ۲ – اقداماتی که اثر حمله احتمالی را کاهش می‌دهد یا آسیب‌پذیری را می‌پوشاند (که در اغلب موارد یک اقدام موقتی است) اغلب اقدامات متقابل یا راه‌کارها[3] نامیده می‌شود.

۳-۷ خدمت

ابزارهایی برای تحویل ارزش به کاربران با آسان‌کردن نتایجی که کاربران می‌خواهند بدون مالکیت منابع فیزیکی یا منطقی خاص به دست آورند و مخاطرات مربوط به مالکیت است.

۳-۸ عرضه‌کننده

فرد یا سازمانی که محصول یا خدمت را توسعه می‌دهد یا مسئول نگهداری آن است.

۳-۹ آسیب‌پذیری

ضعف نرم‌افزار، سخت‌افزار، یا خدمت برخط که می‌تواند مورد بهره‌برداری قرار گیرد.

[بند ۲-۴۶ استاندارد ملی ایران شماره ۲۷۰۰۰ سال ۱۳۹۱.– اصلاح‌شده.]

یادآوری ۱ – ضعف‌های سامانه می‌تواند ناشی از نقص طراحی نرم‌افزار یا سخت‌افزار، فرآیندهای مدیریتی ضعیف، فقدان آگاهی و آموزش، و پیشرفت‌هایی در آخرین فناوری یا بهبودهایی در روش‌های جاری باشد.

۴ کوته‌نوشت‌ها

CCE	Common Configuration Enumeration	شمارش پیکربندی متداول
CPE	Common Platform Enumeration	شمارش بستر متداول
CSIRT	Computer Security Incident Response Team	تیم پاسخگویی رخداد امنیتی رایانه‌ای
CVE	Common Vulnerabilities and Exposures	آسیب‌پذیری‌ها و رخنه‌پذیری‌های متداول
CVSS	Common Vulnerability Scoring System	سامانه امتیازدهی آسیب‌پذیری متداول
ID	identifier	شناسانه
IT	information technology	فناوری اطلاعات
PC	personal computer	رایانه شخصی
PDF	portable document format	قالب سند قابل حمل
PGP	Pretty Good Privacy	حریم کاملا خصوصی

1 - Fix
2 - Hotfix
3 - Workarounds

PoC	proof of concept	اثبات مفهوم
PSIRT	product security incident response team	گروه پاسخگویی رخداد امنیتی محصول
SRM	secure receiving model	مدل دریافت امن
SW	software	نرم‌افزار
URL	uniform resource locator	نشانی وب

۵ مفاهیم

۵-۱ کلیات

هدف این بند این است که اطلاعات پیش‌زمینه و زمینه کاری را فراهم آورد تا به خوانندگان برای درک بهتر مدیریت آسیب‌پذیری و افشای آسیب‌پذیری کمک کند.

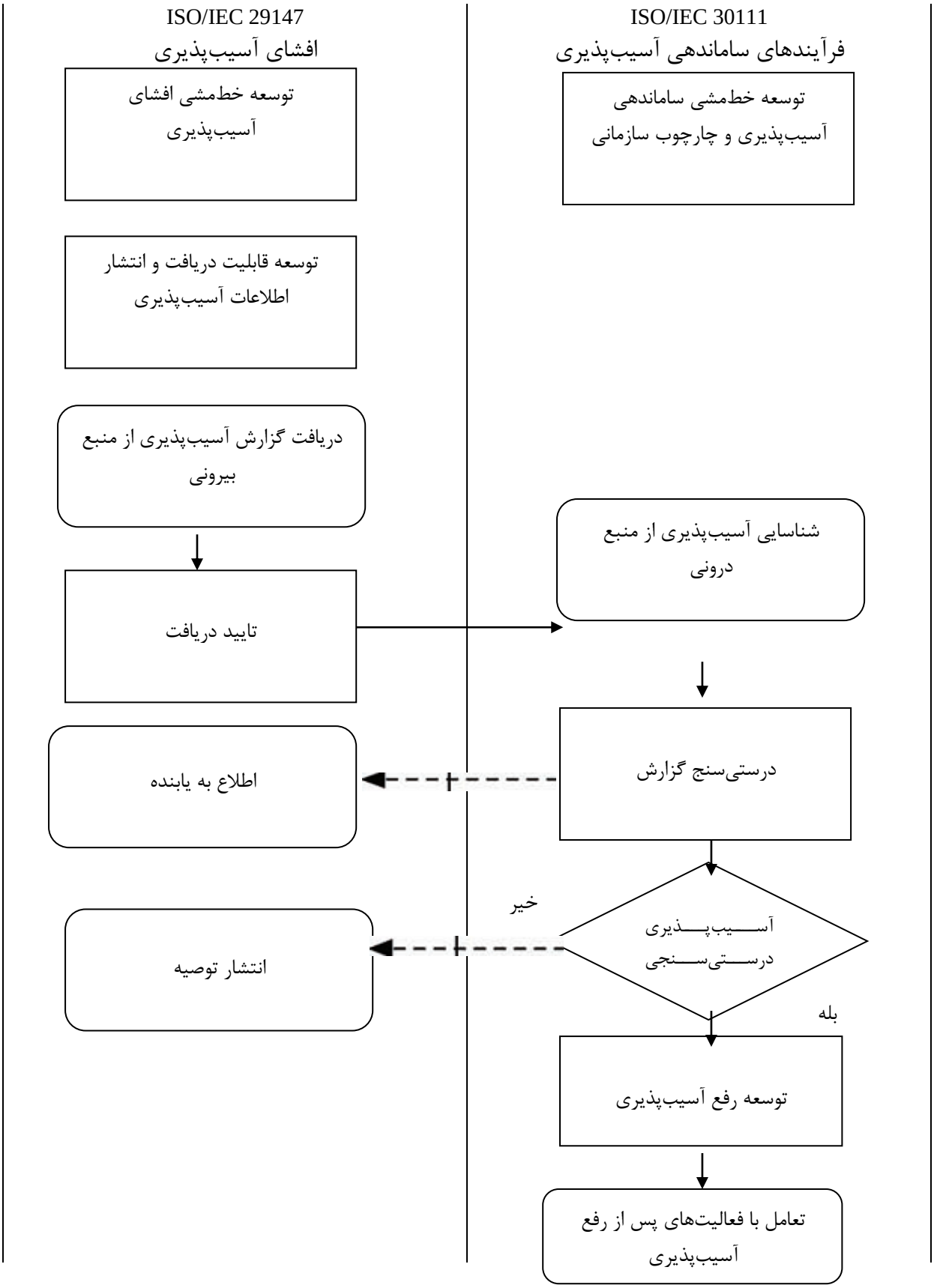
۵-۲ واسط بین ISO/IEC 29147: افشای آسیب‌پذیری و ISO/IEC 30111: فرآیندهای مدیریت آسیب‌پذیری

همان طور که در شکل -۱ نشان داده شده است ISO/IEC 29147: افشای آسیب‌پذیری و ISO/IEC 30111: فرآیندهای مدیریت آسیب‌پذیری استانداردهای مرتبط هستند.

استاندارد ISO/IEC 29147 راهنماهایی را ارائه می‌کند که در فرآیندهای کسب‌وکار عادی عرضه‌کنندگان هنگام دریافت اطلاعات درباره آسیب‌پذیری‌های بالقوه از افراد یا سازمان‌های بیرونی و هنگام توزیع اطلاعات رفع آسیب‌پذیری به کاربران، تحت‌تاثیر قرار گیرد. هدف این استاندارد افراد، اشخاص، کاربران و سازمان‌هایی است که نیازمند روش‌هایی برای دریافت گزارش‌های آسیب‌پذیری و انتشار توصیه‌ها در زمان لازم هستند.

استاندارد ISO/IEC 30111 راهنماهایی را درباره نحوه فرآیندسازی و حل اطلاعات آسیب‌پذیری بالقوه که توسط افراد یا سازمان‌هایی که آسیب‌پذیری بالقوه را در محصول یا خدمت برخط می‌یابند و آن را گزارش می‌کنند، در اختیار قرار می‌دهد. هدف این استاندارد، سازمان‌هایی است که می‌خواهند فرآیندسازی درونی خود را برای مقابله با گزارش‌های دریافت‌شده آسیب‌پذیری قوت بخشند.

ISO/IEC 29147 در رابطه با واسط بین عرضه‌کنندگان و افرادی که آسیب‌پذیری‌های بالقوه را یافته و گزارش می‌کنند، است، اما استاندارد ISO/IEC 30111 در رابطه با بررسی، دسته‌بندی و رفع آسیب‌پذیری‌ها است و به این که منبع آسیب‌پذیری بالقوه از محیط بیرونی عرضه‌کننده یا از تیم‌های امنیتی، توسعه، یا آزمون عرضه‌کننده است، توجه ندارد.



شکل ۱- نگاشت ISO/IEC 29147 و ISO/IEC 30111

۵-۳ محصولات و خدمات برخط

۵-۳-۱ محصولات

محصولات، سامانه‌هایی هستند که توسط عرضه‌کنندگان به منظور فروش یا به صورت رایگان به کاربران ارائه می‌شود. انواع مختلفی از محصولات وجود دارد که نرم‌افزار سفارشی که تحت یک قرارداد برای استفاده پروانه[1] کاربر خاص ایجاد شده، کتابخانه‌هایی که به منظور گنجاده‌شدن در محصولات دیگر ایجاد شده، محصولات آماده مصرف (COTS)[2] برای بازارهای انبوه، پروژه‌های توسعه‌یافته گروهی و محصولات عرضه‌شده تفریحی یا سرگرمی را شامل می‌شود، اما به این موارد محدود نمی‌شود.

در این استاندارد ملی، تمایز میان محصولات سخت‌افزاری و نرم‌افزاری به ندرت مرتبط است. تعداد اندکی از آسیب‌پذیری‌ها به صوت خاص در سامانه‌های سخت‌افزاری وجود دارد. در اکثر موارد، که آسیب‌پذیری‌های سخت‌افزاری نامیده می‌شود، در واقع آسیب‌پذیری در نرم‌افزار سطح پایین یا ثابت‌افزار[3] رخ می‌دهد.

بسته به فروش، توزیع، و مدل‌های پشتیبانی، عرضه‌کنندگان ممکن است فهرستی دقیق از کاربران داشته یا نداشته باشند. این موضوع می‌تواند در زمان اطلاع‌رسانی به کاربرانی که تحت‌تاثیر آسیب‌پذیری هستند، مورد توجه قرار گیرد.

۵-۳-۲ آسیب‌پذیری

آسیب‌پذیری به طور کلی مجموعه‌ای از شرایطی است که نقض خط‌مشی امنیتی آشکار یا ضمنی برای کاربر است. به طور معمول، نقض خط‌مشی امنیتی کاربر، در نتیجه اثر منفی یا ضرر به کاربر است. یک راه مشترک برای دسته‌بندی ضررها، توجه به اثر محرمانگی، یکپارچگی و آسیب‌پذیری دارایی است. برای مثال، آسیب‌پذیری که به مهاجم امکان نصب نرم‌افزار مخرب در سامانه کاربر را می‌دهد، ممکن است از زمان استفاده مهاجم از نرم‌افزار مخرب برای خواندن یا تغییر اطلاعات حساس، به شدت محرمانگی و یکپارچگی را تحت‌تاثیر قرار دهد. آسیب‌پذیری در محصول شبکه که منجر به تجربه خطای سامانه می‌شود، آسیب‌پذیری را تحت‌تاثیر قرار می‌دهد. تاثیر واقعی آسیب‌پذیری به چگونگی استفاده محصول آسیب‌پذیر و عوامل درونی بستگی دارد.

آسیب‌پذیری‌ها اغلب به سبب نقص‌های پیاده‌سازی نرم‌افزار است. آسیب‌پذیری می‌تواند با خط‌مشی امنیتی، در صورت وجود، مرتبط باشد. یک نوع معمول آسیب‌پذیری سرریز بافر و خطاهای مدیریت حافظه سطح پایین مرتبط را شامل می‌شود که به طور خاص به ورودی دستکاری‌شده خاص این امکان را می‌دهد تا اجرای برنامه نرم‌افزاری آسیب‌پذیر را کنترل کند. تزریق SQL و آسیب‌پذیری‌های نبشته سایت قلابی[4] انواع معمولی از آسیب‌پذیری‌ها هستند که در برنامه‌های کاربردی وب یافت می‌شود. بسیاری از مجموعه شرایط دیگر، شامل تصمیمات طراحی، تنظیمات پیکربندی پیش‌فرض، اصالت‌سنجی ضعیف یا کنترل دسترسی کم

1 - license
2 - commercial off-the-shelf
3 - firmware.
4 - cross-site scripting

بودن آگاهی یا آموزش، یا حتی تعاملات غیرقابل انتظار میان سامانه‌ها یا تغییرات در محیط‌های عملیاتی می‌تواند منجر به آسیب‌پذیری شود یا در آن مشارکت داشته باشد.

اطلاعات بیشتر درباره انواع آسیب‌پذیری‌ها می‌تواند در شمارش ضعف مشترک (CWE)[1] و پروژه امنیت برنامه کاربردی وب باز (OWASP)[2] یافت شود. هر دو سازمان CWE و OWASP بر آموزش توسعه‌دهندگان و مهندسین در تهدیدات امنیتی کنونی تمرکز دارند که چگونگی کشف و رتبه‌بندی آنها و این که چگونه به صورت برنامه‌ریزی‌شده کد و برنامه‌های کاربردی بهتری ایجاد کند را شامل می‌شود. پیوندها به این دو وبگاه در بند ب-۴ قرار دارد.

بسیاری از ذینفعان (عمدتاً عرضه‌کنندگان و کاربران) به دنبال شناسایی و حل آسیب‌پذیری‌ها با حذف کامل آنها (به طور معمول با ارائه وصله یا روزآمد کردن[3] نرم‌افزار برای حذف نقص‌ها) یا با کاهش یا کار در حیطه آسیب‌پذیری‌ها هستند تا احتمال و/یا اثر حمله موفق را کاهش دهند. افشای آسیب‌پذیری برای عرضه‌کنندگان و کاربران، اطلاعاتی را فراهم می‌آورد تا آسیب‌پذیری را حل و کاهش دهند و تصمیمات مدیریت مخاطرات بهتری را اتخاذ کنند.

مهاجمان نیز به دنبال شناسایی آسیب‌پذیری‌ها هستند، اما به طور معمول تلاشی برای افشا یا حل آسیب‌پذیری‌ها نمی‌کنند. مهاجمان به دنبال بهره‌برداری از آسیب‌پذیری‌ها برای اهدافی هستند که اغلب منجر به ضرر برای کاربران خواهد شد.

۵-۳-۳ وابستگی درونی محصولات

بسیاری از محصولات، سامانه‌های پیچیده‌ای هستند که به نوعی شامل محصولات دیگر نیز می‌شوند. محصولاتی که می‌تواند از کد منبع سایر محصولات، کتابخانه‌های نرم‌افزاری، یا سایر انواع واسط‌ها استفاده کنند. برخی محصولات به صورت بنیادی مشابه یکدیگر هستند اما تحت نمانام‌های[4] متفاوت و توسط عرضه‌کنندگان متفاوت به فروش می‌رسند. محصولات متفاوتی که از پروتکل شبکه یا قالب پرونده مشابه پشتیبانی می‌کنند، ممکن است تحت‌تاثیر یک آسیب‌پذیری در پروتکل یا قالب قرار گیرند. کاربر یا عرضه‌کننده ممکن است مطمئن نباشد که کدام محصولات تحت‌تاثیر آسیب‌پذیری قرار دارد. این وابستگی درونی، زمانی اهمیت می‌یابد که محصولات مورد استفاده یا محصولات در تعامل با محصول آسیب‌پذیر، نیز ممکن است آسیب‌پذیر باشند.

۵-۴ ذینفعان

این زیربند ذینفعان اصلی در فرآیند افشای آسیب‌پذیری را برمی‌شمرد.

1 - Common Weakness Enumeration
2 - Open Web Application Security Project
3 - Updating
4 - brands

۵-۴-۱ کاربر

کاربران ممکن است به صورت مستقیم با محصولات نرم‌افزاری یا سخت‌افزاری کار کنند یا از یک خدمت برخط استفاده کنند. این افراد ممکن است به عنوان مصرف‌کنندگان، مشتریان، یا کاربران نهایی در نظر گرفته شوند. با توجه به وابستگی متقابل محصولات نرم‌افزاری جدید، کاربران ممکن است ندانند که دقیقا از کدام مولفه‌ها یا محصولات استفاده می‌کنند.

کاربران به اطلاعات درباره آسیب‌پذیری‌ها، به خصوص آموزش نیاز دارند، تا تصمیمات مخاطره موثری را اتخاذ کنند و از محصولات نرم‌افزاری و خدمات برخط به صورت ایمن‌تر استفاده کنند. فراهم آوردن اطلاعات آسیب‌پذیری برای کاربران در بند ۹ مورد بحث قرار گرفته است.

۵-۴-۲ عرضه‌کننده

عرضه‌کننده، محصول یا خدمت برخط را توسعه می‌دهد یا مسئول نگهداری آن است. عرضه‌کننده ممکن است فرد یا سازمان همچون یک کسب‌وکار تجاری یا یک پروژه منبع باز باشد. اصطلاحات متفاوت زیادی برای توصیف افراد یا سازمان‌هایی که محصولات نرم‌افزاری را به صورت آزاد تحویل می‌دهند، وجود دارد که شامل توسعه‌دهنده، نگهدارنده، یا توزیع‌کننده می‌شود. به طور مشابه، فرد یا سازمانی که محصولات نرم‌افزاری را در یک زنجیره تامین تحویل می‌دهد، ممکن است تامین‌کننده نامیده شود. در این استاندارد ملی، اصطلاح «عرضه‌کننده» برای تمامی این موارد به کار می‌رود.

عرضه‌کنندگان، مسئول کیفیت محصولات و خدمات برخط خود هستند. عرضه‌کنندگان از افشای آسیب‌پذیری برای یادگیری آسیب‌پذیری‌ها به منظور توسعه اقدامات رفع و کاهش آسیب‌پذیری و توزیع اطلاعات بین کاربران استفاده می‌کنند.

انواع زیادی از عرضه‌کنندگان با مدل‌های مختلف توسعه، فروش، پشتیبانی و توزیع محصولات وجود دارد. برخی عرضه‌کنندگان، محصولات را در یک سامانه یا خدمت تجمیع می‌کنند و این عرضه‌کنندگان ممکن است به عنوان مشتریان یا کاربران محصولات مولفه ایفای نقش کنند. این عرضه‌کنندگان میانی ممکن است به عرضه‌کنندگان مولفه به اطلاعات رفع و کاهش آسیب‌پذیری وابسته باشند.

۵-۴-۳ عرضه‌کننده میانی

عرضه‌کننده میانی، زیرسامانه‌ای را از عرضه‌کننده می‌گیرد و از آن برای تامین سامانه یا خدمت (یا ترکیبی از هر دو) برای کاربر (یا عرضه‌کننده میانی دیگر) استفاده می‌کند. مثال‌های نمونه به شرح زیر است:

الف) خانه‌های سامانه‌ای که از رایانه شخصی و سامانه‌عامل برای اضافه‌کردن نرم‌افزار مدیریت مراقبت سلامت خود استفاده می‌کند و سامانه ترکیبی را به پزشک می‌فروشد (شاید به همراه قرارداد نگهداری)؛

ب) ارائه‌کنندگان مخابراتی که تلفن همراه را با یک قرارداد خدمت تامین می‌کنند.

این عرضه‌کنندگان میانی ممکن است در مورد گزارش‌های خطای آسیب‌پذیری‌ها از مشتریان و سرمایه‌گذاران اولیه مطالبی بیاموزند (برای مثال بخشی از کنترل‌های کیفیت برای کالاهای ورودی).

عرضه‌کنندگان میانی باید آسیب‌پذیری‌ها را به عرضه‌کنندگان خود گزارش کنند. مشکل مهم برای عرضه‌کنندگان میانی این است که ممکن است آنها در موقعیتی نباشند که بتوانند برای حل مشکل و حذف آسیب‌پذیری منتظر بمانند.

عرضه‌کنندگان میانی برای آگاه‌سازی مشتریان خود مسئولیتی قانونی دارند، همان طور که مشتریان ممکن است به توقف استفاده از افزاره یا برخی کارکردهای آن یا کار در رابطه با آسیب‌پذیری‌ها برای کاهش مخاطره نیاز داشته باشند. این موضوع به طور خاص زمانی ادامه می یابد که عرضه‌کننده زمان زیادی را برای حذف آسیب‌پذیری صرف کند یا این که اصلاً قادر به انجام این کار نباشد. در صورتی که عرضه‌کننده میانی، مشتری خودش را آگاه سازد، به این معنی است که آسیب‌پذیری قبل از این که عرضه‌کننده قادر به مقابله با آن باشد، افشا شده است.

عرضه‌کنندگان میانی ممکن است همچنین به صورت فنی قادر به تولید و توزیع راه‌کارها برای کمینه حفاظت از استفاده محصول یا خدمت خود یا حتی پیکربندی خاص سامانه اصلی باشند (برای مثال پیکربندی محدودکننده سامانه عامل). نقش آنها به عنوان رابط، این عرضه‌کنندگان را در جایگاهی قرار می‌دهد که مجبور به تعامل پایاپای هستند (برای مثال آگاه‌سازی سریع مشتریان در مورد آسیب‌پذیری‌ها در مقابل راه‌حل‌های ارتباطی برای مشکلات).

۵-۴-۴ یابنده

یابنده، فرد یا سازمانی است که آسیب‌پذیری بالقوه را در محصول یا خدمت برخط شناسایی می‌کند. یابنده اغلب محقق امنیت یا آسیب‌پذیری است. همچنین یابنده ممکن است کاربر یا عرضه‌کننده باشد. در این استاندارد، انتظار می‌رود که یابنده برای اطلاع‌رسانی به عرضه‌کننده یا هماهنگ‌کننده در مورد آسیب‌پذیری تلاش کند. در عمل، یابنده ممکن است به صورت اختیاری تلاشی برای آگاه سازی عرضه‌کننده یا هماهنگ‌کننده نکند یا این که تلاش او بی ثمر باشد. دریافت اطلاعات آسیب‌پذیری از یابندگان در بند ۷ بحث شده است.

۵-۴-۵ هماهنگ‌کننده

هماهنگ‌کنندگان ممکن است با دیگر هماهنگ‌کنندگان کار کنند تا به کمک و به اشتراک‌گذاری تلاش خود با متخصص دامنه، زبان، زمان محلی و موانع فرهنگی دست یابند. برخی تیم‌های پاسخ به رخداد امنیتی رایانه‌ای (CSIRT)[1] خدمات هماهنگی آسیب‌پذیری را بر پایه‌ای عملیاتی فراهم می‌آورند و سایر تیم‌های پاسخ به رخداد امنیتی رایانه‌ای به موارد انفرادی هماهنگی کمک می‌کنند. برخی عرضه‌کنندگان همچنین خدمات هماهنگی را ارائه می‌کنند.

خدمات متداول که توسط یک هماهنگ‌کننده ارائه می‌شود شامل موارد زیر است:

- کمک به یابندگان برای شناسایی و تماس با عرضه‌کنندگان؛

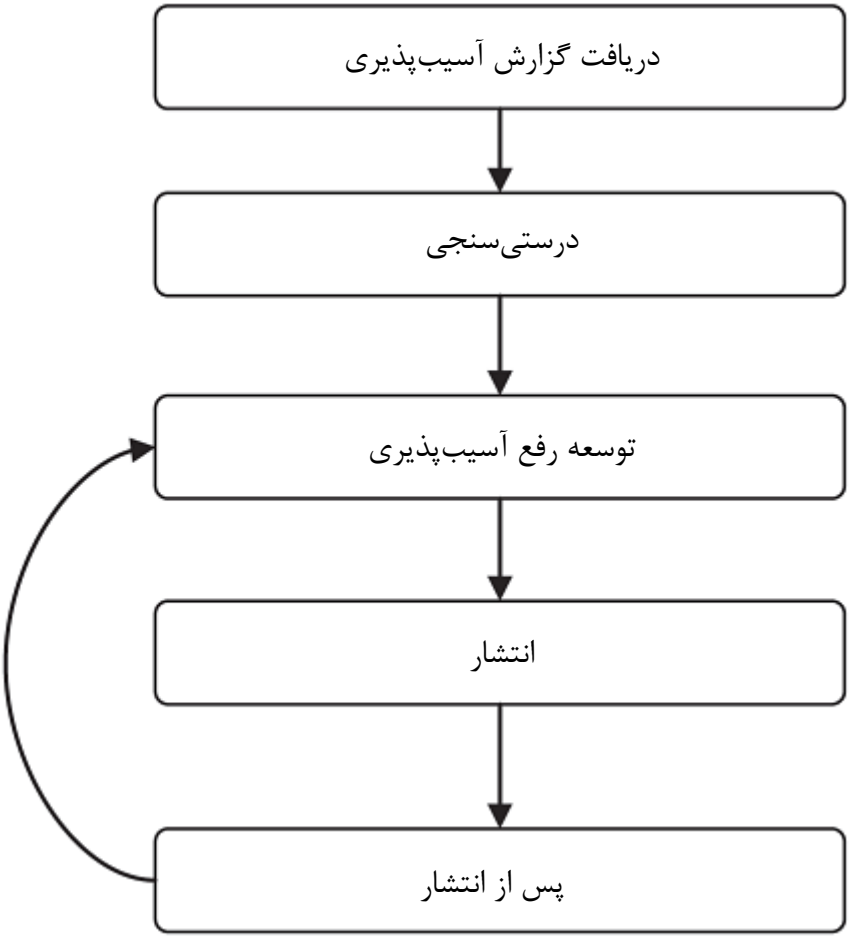
1 - Computer Security Incident Response Teams

- هماهنگ‌کردن آسیب‌پذیری‌هایی که چندین عرضه‌کننده را تحت‌تاثیر قرار می‌دهد؛
- انجام تحلیل فنی و اعتبارسنجی گزارش‌های آسیب‌پذیری؛ و
- انتشار توصیه‌ها

درحالی که هماهنگ‌کنندگان اغلب، راغب به محافظت از مشتریان خود هستند، هماهنگ‌کنندگان باید تلاش کنند تا به صورت فنی بی طرف باشند و مخاطره را برای همه ذینفعان کمینه کنند.

۵-۵ خلاصه فرآیند افشای آسیب‌پذیری

این زیربند فرآیند افشای آسیب‌پذیری را خلاصه می‌کند که در استاندارد ISO/IEC 30111 موجود است. شکل – ۲ فرآیند افشای آسیب‌پذیری عرضه‌کننده را ترسیم می‌کند که شامل ۵ گام سطح بالا است.



شکل ۲- خلاصه فرآیند افشای آسیب‌پذیری

۵-۵-۱ مرحله دریافت گزارش آسیب‌پذیری

یابنده آسیب‌پذیری‌های بالقوه در محصولات و خدمات برخط را شناسایی و به عرضه‌کننده گزارش می‌کند. عرضه‌کننده دریافت گزارش را تایید می‌کند.

۵-۵-۲ مرحله درستی‌سنجی

عرضه‌کننده گزارش را بررسی می‌کند. بررسی اغلب تلاش برای بازتولید محیط و رفتار گزارش‌شده توسط یابنده را در برمی‌گیرد. این امر ممکن است یک بررسی اولیه باشد که در ابتدا بر نیاز به تلاش بیشتر توسط عرضه‌کننده تمرکز می‌کند. بررسی ممکن است همچنین شامل همبستگی مشابه یا گزارش‌های مرتبط، ارزیابی شدت و تعیین دیگر محصولات تحت‌تاثیر باشد. این بررسی تعیین می‌کند که آیا گزارش شامل آسیب‌پذیری می‌شود یا خیر. عرضه‌کننده ممکن است با یابنده در طول بررسی ارتباط برقرار کند و نتایج را در پایان بررسی به یابنده اعلام کند.

۵-۵-۳ مرحله توسعه رفع آسیب‌پذیری

عرضه‌کننده، رفع آسیب‌پذیری‌های گزارش‌شده توسط یابنده را توسعه می‌دهد. توسعه رفع آسیب‌پذیری ممکن است بررسی با جزئیات علت ریشه‌ای آسیب‌پذیری‌ها و تعیین سایر محصولاتی که توسط همان آسیب‌پذیری‌ها یا آسیب‌پذیری‌های مشابه تحت‌تاثیر هستند را در برداشته باشد. عرضه‌کننده به طور معمول فنون آموزش و کاهش آسیب‌پذیری را توسعه می‌دهد و آزمون‌های مثبت را برای تعیین این که آموزش به درستی کار می‌کند و آزمون‌های منفی (رگرسیون) را برای اطمینان از این که آموزش مشکلی در کارکرد موجود ایجاد نمی‌کند، انجام می‌دهد.

۵-۵-۴ مرحله انتشار

عرضه‌کننده آموزش را گسترش می‌دهد. عرضه‌کننده آموزش و مستندات رویداد را در یک خدمت برخط، مستقر می‌کند. برای محصول، عرضه‌کننده اطلاعات آموزشی و کاهش آسیب‌پذیری را به طور معمول به شکل توصیه آسیب‌پذیری و وصله‌ها و روزآمد های نرم‌افزاری برای کاربران فراهم می‌آورد و کاربران آموزش را به کارمی‌گیرند. عرضه‌کننده ممکن است توصیه را قبل از این که آموزش در دسترس باشد، به‌خصوص در موارد بهره‌برداری مثبت یا بحث عمومی، منتشر کند. عرضه‌کننده باید در صورت امکان تلاش کند تا از این که آموزش منجر به معرفی آسیب‌پذیری‌های جدید، مسائل کیفیت کلی محصول، یا مشکلات سازگاری با دیگر محصولات یا خدمات نمی‌شود، اطمینان حاصل کند.

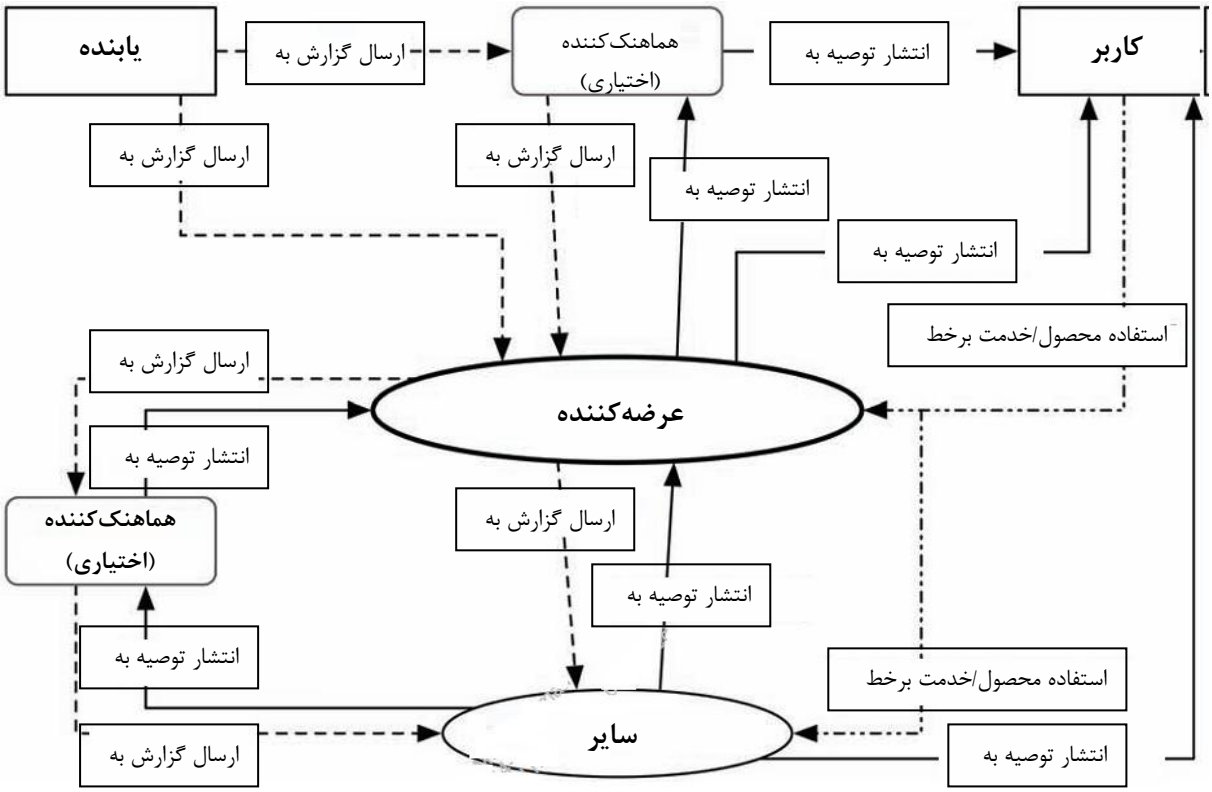
۵-۵-۵ مرحله پس از انتشار

عرضه‌کننده بازخوردهای کاربران را جمع آوری می‌کند و اطلاعات آموزش و کاهش آسیب‌پذیری را در صورت نیاز روزآمد می‌کند. برای مثال، آموزش ممکن است ناقص باشد یا این که منجر به بروز مشکلات بازگشتی یا جانبی شود.

۵-۶ تبادل اطلاعات در طی افشای آسیب‌پذیری

شکل ۳ تبادل اطلاعات را در طی فرآیند افشای آسیب‌پذیری نشان می‌دهد. دو مرحله مهم تبادل وجود دارد: گزارش‌های آسیب‌پذیری بالقوه از طرف یابندگان به عرضه‌کنندگان و توصیه‌های عرضه‌کنندگان به کاربران. گزارش آسیب‌پذیری بالقوه از طرف یابنده به عرضه‌کننده چه به صورت مستقیم یا از طریق هماهنگ‌کنندگان ارسال می‌شود. عرضه‌کننده ممکن است نقش یابنده را ایفا کند و آسیب‌پذیری را به

عرضه‌کننده دیگر گزارش کند. توصیه توسط عرضه‌کننده چه به صورت خصوصی به کاربران خود یا به صورت عمومی منتشر می‌شود. این استاندارد ملی بر روی این دو تبادل از منظر عرضه‌کننده دریافت‌کننده گزارشات آسیب‌پذیری و انتشار اطلاعات آموزش تمرکز می‌کند.



شکل ۳- تبادل اطلاعات آسیب‌پذیری

۵-۷ محرمانگی اطلاعات تبادل‌شده

از آنجایی که اطلاعات آسیب‌پذیری ممکن است برای حمله به محصولات و خدمات برخط آسیب‌پذیر استفاده شود، اطلاعات حساس آسیب‌پذیری باید به صورت محرمانه تبادل شود. عرضه‌کنندگان ممکن است خواستار روش‌های محرمانه امن جهت گزارش اطلاعات آسیب‌پذیری برای یابندگان باشند. یکپارچگی پیام نیز اهمیت دارد، به‌خصوص در درستی‌سنجی که اطلاعات آموزش موثق است. پروتکل‌های رمزگذاری مشترک مانند لایه دریچه امن (SSL)[1]، افزونه‌های پیام اینترنتی چندمنظوره امن (S/MIME)[2] و محرمانگی سطح بالا (PGP)[3] می‌توانند محرمانگی و یکپارچگی را فراهم آورند. در صورت وجود سایر الزامات امنیتی، استاندارد ISO/IEC 27010 ممکن است مرتبط باشد. به طور مثال اگر هماهنگ‌کننده خواستار ارائه پیشنهاد به یابنده در مورد خدمت گمنام باشد.

۵-۸ توصیه‌های آسیب‌پذیری

1 - Secure Sockets Layer
2 - Secure Multipurpose Internet Mail Extensions
3 - Pretty Good Privacy

اطلاعات آسیب‌پذیری به صورت کلی در یک توصیه منتشر می‌شود. توصیه آسیب‌پذیری را به صورت معمول با تمرکز بر آموزش و کاهش آسیب‌پذیری توصیف می‌کند، اما همچنین شامل اطلاعاتی در مورد سامانه‌های تحت‌تاثیر، حمله‌ها، اثر و مراجع مرتبط می‌شود. کاربران با مطالعه توصیه به اطلاعات کافی جهت اتخاذ تصمیمات مخاطره‌ساز در مورد چگونگی آموزش یا کاهش آسیب‌پذیری نیاز دارند.

کاربران باید قادر به درستی‌سنجی رمزنگاری اصالت و یکپارچگی توصیه و آموزش (به خصوص وصله‌ها و روزآمد ها) باشند.

۵-۹ بهره‌برداری از آسیب‌پذیری

به طور کلی، مهاجمان به دنبال بهره‌برداری از آسیب‌پذیری‌ها برای کسب منافع هستند که تقریبا همیشه منجر به زیان کاربران می‌شود. عوامل مختلفی مانند جامعه هدف، اهداف رخنه‌پذیری، ارزش اهداف برای مهاجمان و هزینه توسعه بهره‌برداری می‌تواند بر این که آیا آسیب‌پذیری توسط مهاجمان مورد بهره‌برداری قرار می‌گیرد یا خیر تاثیر بگذارد. هر تلاشی، به هر اندازه، برای پیشگویی این که آیا آسیب‌پذیری در حال حاضر در حملات مورد استفاده قرار گرفته یا خواهد گرفت، کاملا غیرقطعی است. بیشترین فرض محتاطانه این است که آسیب‌پذیری در حملات می‌تواند استفاده شود و خواهد شد (و ممکن است قبلا استفاده شده باشد).

۶ ملاحظات خط‌مشی افشای آسیب‌پذیری

۶-۱ کلیات

این بند در مورد ملاحظاتی که باید در زمان ایجاد تدبیر افشای آسیب‌پذیری برشمرده شوند، بحث می‌کند. هر عرضه‌کننده الزامات و منابع در دسترس مختلفی برای کار با اطلاعات آسیب‌پذیری امنیتی دارد.

عرضه‌کنندگان باید مسئولیت‌های خود را در خط‌مشی افشای آسیب‌پذیری تعریف کنند و باید خط‌مشی افشای آسیب‌پذیری را به اطلاع عموم رسانده یا به خط‌مشی افشای آسیب‌پذیری اشاره کنند. مثال‌های بسیاری در بند ب-۱ فهرست شده است.

خط‌مشی افشا باید اهداف عرضه‌کننده و مسئولیت‌هایش و همچنین انتظار عرضه‌کننده از ذینفعان را بیان کند. خط‌مشی افشای آسیب‌پذیری باید ساده و شفاف باشد تا گزارش‌دهی آسان آسیب‌پذیری‌های محصول را برای عرضه‌کننده امکان‌پذیر کند. عرضه‌کنندگان باید به جایگزین شهودی اطلاعات مرتبط با امنیت محصول توجه کنند. چنین محلی ممکن است یک صفحه وب امنیتی باشد (مانند www.example.com/security).

۶-۲ کمینه جوانب خط‌مشی

عرضه‌کننده باید خط‌مشی کلی افشای آسیب‌پذیری را ایجاد کند، اما در صورتی که خط‌مشی داخلی شامل اطلاعات حساس باشد، ممکن است فقط بخش‌های انتخاب‌شده را به اطلاع عموم برساند.

الف) عرضه‌کننده مایل است چگونه قرارداد ببندد

عرضه‌کنندگانی که خط‌مشی افشای آسیب‌پذیری را می‌پذیرند، به طور معمول یک وبگاه یا صفحه امنیتی پیشنهاد می‌دهند. این صفحه/ وبگاه برای دریافت اطلاعات آسیب‌پذیری از یابنده، اطلاعاتی در مورد روش(های) مورد قبول عرضه‌کننده ارائه می‌کند.

اطلاعات تماس ممکن است شامل یک یا تعداد بیشتری از موارد ذیل باشد:

۱) نشانی رایانامه؛

مثال‌هایی از رایانامه مستعار که می‌تواند مورد استفاده قرار بگیرد، شامل موارد ذیل است:

- Security-alert@example.com
- security@example.com
- secure@example.com
- psirt@example.com
- csirt@example.com

۲) شماره تماس

۳) فرم وب

عرضه‌کنندگان می‌توانند یک فرم وب را پیشنهاد دهند که یابنده باید آن را تکمیل کند. این کار این مزیت را دارد که عرضه‌کننده می‌تواند اطلاعات اختیاری و اجباری را از یکدیگر متمایز کند و فرآیند ورود داده در پایگاه‌داده آسیب‌پذیری را خودکار سازد.

ب) گزینه‌های ارتباط امن

به دلیل جنبه مخاطره پیام‌های متنی شفاف، عرضه‌کنندگان باید یک کانال ارتباطی امن را فراهم سازند. این کار می‌تواند نفوذ فناوری‌هایی مانند S/MIME یا PGP را برای اطمینان از حفاظت تبادل اطلاعات باشد. همچنین عرضه‌کنندگان می‌توانند درگاه‌های وب با استفاده از پروتکل انتقال ابرمتن امن (HTTPS)[1] را برای ارائه گزارش آسیب‌پذیری پیشنهاد دهند. عرضه‌کنندگان باید این قابلیت‌ها را قبل از برقراری ارتباط با یابندگان پیکربندی کنند.

پ) تنظیم انتظارات ارتباطی

عرضه‌کنندگان باید انتظارات برای ارتباط، شامل تایید اولیه دریافت گزارش و روزآمد های وضعیت را توضیح دهند/ تنظیم کنند. عرضه‌کنندگان باید روزآمد ها را با استفاده از روش مورد توافق ارتباطی برای یابنده فراهم کنند.

ت) اطلاعاتی که زمان ارائه گزارش آسیب‌پذیری احتمالی مفید است.

1 - Hypertext Transfer Protocol Secure

مهم است که عرضه‌کنندگان مکالمه باز و همکارانه را با یابندگان حفظ کنند تا اطلاعات در مورد آسیب‌پذیری‌ها به اشتراک گذاشته شود و مخاطره برای کاربران تا حد ممکن کاهش یابد. زمانی که یابنده تماسی را به موجب یک آسیب‌پذیری بالقوه برقرار می‌کند، عرضه‌کنندگان باید تعیین کنند که آیا یابنده اطلاعات کافی را برای تائید یا رد مسئله ارائه کرده است یا خیر. این موضوع در هر وضعیتی متفاوت است. بند الف-۲ مثال‌هایی از اطلاعات مفید برای عرضه‌کنندگان را فهرست کرده است. اگر عرضه‌کننده تعیین کند که یابنده اطلاعات کافی ارائه نکرده است، عرضه‌کننده ممکن است با یابنده برای درخواست جزئیات بیشتر تماس بگیرد. عرضه‌کنندگان میانی ممکن است خواستار اطلاعاتی باشند که می‌تواند نشان دهد عرضه‌کننده پایانی یا سایر عرضه‌کنندگان میانی منبع آسیب‌پذیری هستند و ممکن است یابنده، آسیب‌پذیری را به آنها گزارش کرده باشد.

ث) خدمات خارج از محدوده

در اغلب موارد، تیمی که با گزارش‌های آسیب‌پذیری سروکار دارد قادر به کار با رخدادهای امنیتی و دیگر سوالات مرتبط امنیتی نیست. عرضه‌کنندگان باید نقاط تماسی را برای این نوع درخواست‌ها مشخص کنند.

عرضه‌کننده ممکن است خواستار ارائه پیشنهاداتی برای ارائه اطلاعات بیشتر باشد که ممکن است برای درک آسیب‌پذیری و آموزش‌های ممکن مفید باشد. عرضه‌کننده ممکن است فراهم کردن یک فرم برای این منظور را مورد توجه قرار دهد.

در مواردی که آسیب‌پذیری بر چندین عرضه‌کننده تاثیر می‌گذارد، مفید است تا عرضه‌کنندگان بدانند آیا یابنده نیز آسیب‌پذیری را به دیگر عرضه‌کنندگان تحت‌تاثیر گزارش کرده است یا خیر.

ج) چگونه گزارش‌های ارائه‌شده ردیابی می‌شوند

عرضه‌کننده باید ابزارهایی را برای ردیابی اطلاعات دریافتی درباره اطلاعات آسیب‌پذیری احتمالی تعریف کند و با آن روش با یابندگان در ارتباط باشد.

۶-۳ جوانب خط‌مشی اختیاری

خط‌مشی افشای آسیب‌پذیری ممکن است شامل مولفه‌های اختیاری چندگانه باشد.

الف) اعتبار به یابنده

عرضه‌کننده ممکن است از مشارکت‌های یابندگانی که در کشف یا پیشبرد رفع آسیب‌پذیری کشف‌شده کمک کرده‌اند، قدردانی کند. قبل از انجام این کار عرضه‌کننده باید مطمئن شود که این قدردانی خوشایند یابنده باشد.

ب) افشای عمومی همزمان

در صورتی که آموزش‌ها در دسترس باشد، عرضه‌کننده و یابنده ممکن است به افشای عمومی همزمان و مشترک برسند.

پ) توزیع

عرضه‌کننده ابزاری را برای انتشار توصیه‌های امنیتی پیشنهاد می‌دهد که ممکن است شامل یک وبگاه، فهرست ارسال رایانامه و غیره، شامل اطلاعاتی در مورد چگونگی اشتراک یا عدم اشتراک باشد.

۷ دریافت اطلاعات آسیب‌پذیری

۷-۱ کلیات

این بند، راهنماهایی برای عرضه‌کنندگان در زمان دریافت اطلاعات آسیب‌پذیری‌های بالقوه از عرضه‌کننده یا هماهنگ‌کننده‌ای که به عرضه‌کنندگان کمک می‌کنند، ارائه می‌دهد.

الف) اطمینان حاصل کنید که تیم آنها در قبال ساماندهی آسیب‌پذیری مسئول است و می‌تواند گزارش‌های آسیب‌پذیری را با سرعت و به صورت امن تا حد ممکن دریافت کند، و

ب) یک رابطه کاری را بین یابنده یا هماهنگ‌کننده برقرار و حفظ کنید.

۷-۲ گزارش آسیب‌پذیری بالقوه و مدل دریافت امن آن

گزارش‌های آسیب‌پذیری بالقوه به عرضه‌کنندگان یا هماهنگ‌کنندگان توسط یابندگان ارسال می‌شود تا فرآیند ساماندهی آسیب‌پذیری به سرعت آغاز شود. این گزارش‌ها شامل توصیف این که کدام محصول یا خدمت برخط آسیب‌پذیری بالقوه دارد و چگونه آسیب‌پذیری بالقوه بروز می‌کند. گزارش‌ها ممکن است شامل کد اثبات مفهوم (PoC)[1] باشد که نشان‌دهنده بهره‌برداری از آسیب‌پذیری است. از آنجایی که گزارش آسیب‌پذیری ممکن است شامل اطلاعات حساسی مانند کد PoC باشد، عرضه‌کننده باید ابزارهایی برای دریافت اطلاعات به صورت امن فراهم کند.

۷-۳ تایید دریافت از یابنده یا هماهنگ‌کننده

عرضه‌کننده باید به گزارش آسیب‌پذیری در مدت زمانی که در خط‌مشی افشای آسیب‌پذیری عرضه‌کننده مشخص شده است، پاسخ دهد. توصیه می‌شود که تایید دریافت گزارش آسیب‌پذیری به یابنده در طول هفت روز تقویمی انجام شود.

۷-۴ گزارش‌های ورودی ردیابی

عرضه‌کننده باید یک سامانه ردیابی داشته باشد که برای ثبت و ردیابی کلیه گزارش‌های آسیب‌پذیری‌های بالقوه از آن استفاده شود. باید امکان ردیابی بدون ابهام هر گزارش وجود داشته باشد. این تخصیص می‌تواند توسط عرضه‌کننده، عرضه‌کننده میانی، یابنده، هماهنگ‌کننده یا هر طرف سومی که در فرآیند افشای آسیب‌پذیری نقش دارد، انجام شود.

به منظور ردیابی، عرضه‌کننده باید یک شناسانه داخلی منحصر به فرد را به گزارش آسیب‌پذیری بالقوه تخصیص دهد. بهتر است از این شناسانه منحصر به فرد در تمامی ارتباطات ذینفعان در ارزیابی آسیب‌پذیری

1 - Proof-of-concept

استفاده شود. یابندگان همچنین می‌توانند یک شناسانه داخلی را تخصیص دهند که می‌تواند در فرآیند ردیابی عرضه‌کننده قرار داشته باشد.

۷-۵ ارتباط مستمر با یابنده

عرضه‌کنندگان باید مسئله گزارش‌شده را ارزیابی کنند و تعیین کنند که آیا آسیب‌پذیری را نشان می‌دهد یا خیر. عرضه‌کننده باید یابنده و هماهنگ‌کننده را در صورت سروکار داشتن با موضوع، از نتایج حاصل مطلع کند.

عرضه‌کننده میانی باید وارسی کند که آیا می‌تواند به تنهایی در مورد آسیب‌پذیری بالقوه تصمیم بگیرد، یا نیاز دارد تا با عرضه‌کننده‌ای که زیرسامانه مرتبط را دارد در ارتباط باشد. در صورتی که نیاز باشد عرضه‌کننده دیگری در تصمیم مشارکت کند و در صورتی که این کار پاسخ را به تاخیر بیاندازد. عرضه‌کننده میانی باید یابنده و/یا هماهنگ‌کننده را در مورد این واقعیت و فرآیندسازی بیشتر مطلع کند.

۷-۶ اطلاعات جزئی

در حین سرمایه‌گذاری، عرضه‌کننده ممکن است اطلاعات کافی برای رسیدن به یک برآورد کامل آسیب‌پذیری را در دست نداشته باشد. در این مورد، عرضه‌کننده باید از یابنده درخواست کند، ورودی بیشتری را با استفاده از کانال‌های ارتباطی مورد توافق فراهم کند.

ارتباط تکمیلی بین عرضه‌کننده و یابنده با استفاده از روش‌های مورد توافق انجام می‌شود. یکی از موارد ممکن، فرم وب است. مثال‌هایی از این فرم‌های وب در بند الف-۳ نشان داده شده است.

۷-۷ پشتیبانی از هماهنگ‌کنندگان

هماهنگ‌کنندگان می‌توانند نقش‌های چندگانه زیر را در فرآیند افشای آسیب‌پذیری ایفا کنند.

الف) ایفای نقش به عنوان رابط مورد اعتماد بین طرف‌هایی که با موضوع سروکار دارند

ب) هماهنگ کردن تاریخ‌های انتشار عمومی توصیه‌ها

پ) فعال کردن ارتباط بین طرف‌هایی که با موضوع سروکار دارند (عرضه‌کنندگان و یابندگان)

ت) ارائه کردن محیط یا انجمنی که در آنجا متخصصان سازمان‌های مختلف بتوانند در بحث در مورد آسیب‌پذیری مشارکت کنند.

انتخاب هماهنگ‌کننده می‌تواند به عواملی مانند همجواری جغرافیایی، زبان و مدل عملیاتی مورد قبول بستگی داشته باشد.

در مواردی که چندین عرضه‌کننده تحت‌تاثیر یک آسیب‌پذیری هستند، عرضه‌کنندگان باید برای هماهنگ کردن زمان انتشار توصیه خود چه به صورت مستقیم یا با کمک هماهنگ‌کننده تلاش کنند. عرضه‌کننده ممکن است درخواست کند که هماهنگ‌کننده، شناسه CVE را فراهم یا خریداری کند. در برخی موارد،

بیشتر از یک هماهنگ‌کننده می‌توانند شامل شوند. عرضه‌کنندگان می‌توانند پیشنهاد کنند که هماهنگ‌کننده نقش سرگروه را ایفا کند تا پیچیدگی و نابسامانی کاهش پیدا کند.

۸ گزارش‌دهی آسیب‌پذیری احتمالی در میان عرضه‌کنندگان

۸-۱ کلیات

به عنوان نتیجه بررسی با جزئیات آسیب‌پذیری گزارش‌شده، عرضه‌کننده می‌تواند بیابد که این آسیب‌پذیری توسط برخی مولفه‌ها یا تحت‌تاثیر بستری که عرضه‌کننده دیگری تامین می‌کند بروز پیدا کرده و آسیب‌پذیری مربوط به کدام یک را نمی‌تواند حل کند. به‌علاوه، عرضه‌کنندگان گاهی اوقات با وضعیت‌هایی برخورد می‌کنند که برای گزارش آسیب‌پذیری‌ها به دیگر عرضه‌کنندگان مطلوب آنها است. این بخش توصیف می‌کند که چگونه گزارش‌دهی آسیب‌پذیری در میان عرضه‌کنندگان باید انجام شود.

۸-۲ موارد نمونه میان عرضه‌کنندگان جهت گزارش آسیب‌پذیری

موارد نمونه‌ای که عرضه‌کننده می‌تواند اطلاعات آسیب‌پذیری را به دیگر عرضه‌کنندگان گزارش کند شامل موارد زیر است:

الف) زمانی که عرضه‌کننده باور دارد آسیب‌پذیری در محصول یا خدمت برخط آنها توسط مولفه یا ابزاری ناشی شده که دارای پروانه استفاده توسط عرضه‌کننده دوم است.

ب) زمانی که آسیب‌پذیری با روشگان یا بینش جدیدی شناسایی شده و بسیاری از دیگر عرضه‌کنندگان محصولات و خدمات برخط همان دسته، هچنین باور دارند که آسیب‌پذیر هستند.

پ) زمانی که آسیب‌پذیری در پروتکل یا قالب پشتیبانی‌شده توسط سایر محصولات و خدمات برخط عرضه‌کننده تعریف شده است.

گرچه، اولین عرضه‌کننده می‌تواند سایر عرضه‌کنندگان را شناسایی کند که به کدام یک باید گزارش اطلاعات آسیب‌پذیری را ارائه دهد، اما این موضوع نمی‌تواند در همه موارد ممکن باشد. حتی در مواردی که عرضه‌کننده می‌تواند شناسایی شود، شناسایی نقطه تماس مناسب ممکن نیست (به طور مثال مورد نرم‌افزار متن باز). این موارد می‌توانند با درخواست پشتیبانی از هماهنگ‌کنندگان به صورت موثر ساماندهی شود.

۸-۳ گزارش‌دهی اطلاعات آسیب‌پذیری به سایر عرضه‌کنندگان

عرضه‌کننده می‌تواند گزارش اطلاعات آسیب‌پذیری را به سایر عرضه‌کنندگان به صورت مستقیم یا غیرمستقیم از طریق هماهنگ‌کنندگان به همان روشی که یابنده آسیب‌پذیری را بالقوه را به عرضه‌کننده گزارش می‌کند، ارائه دهد. در این مورد، عرضه‌کننده ممکن است همچنین آنها را از مواردی آگاه سازد که آسیب‌پذیری با محصول یا خدمت برخط او مرتبط است و از سایر عرضه‌کنندگان درخواست کند که رفع آسیب‌پذیری را قبل از افشای عمومی ارائه دهند تا افشای آسیب‌پذیری با دیگر عرضه‌کننده(ها) همزمان شود.

۹ انتشار توصیه

۹-۱ کلیات

این بند در مورد جوانب انتشار توصیه بحث می‌کند. عرضه‌کنندگان در این مرحله وجود آسیب‌پذیری را تائید کرده‌اند و برای انتشار اطلاعات جهت کمک به آموزش کاربران تحت‌تاثیر از مخاطره مرتبط، آماده هستند.

۹-۲ هدف از توصیه

توصیه، اطلاعاتی در مورد آسیب‌پذیری ارائه می‌کند و باید شامل اطلاعاتی در مورد مخاطره بر اساس بهره‌برداری موفق و چگونگی کاهش آن باشد.

۹-۳ ملاحظات در افشای توصیه

موارد زیر باید در تدوین فرآیند برای تولید و توزیع توصیه‌ها مورد توجه قرار گیرد.

الف) هر طرفی که اطلاعات آسیب‌پذیری را به عنوان توصیه، تولید و توزیع می‌کند، باید نیازهای خوانندگان آینده را در نظر بگیرد. محتوا باید هم در محتوای اطلاعاتی و هم قالب‌های توزیع، مناسب و موثر باشد. قالب‌های توزیع در بند ۹-۷ بیشتر توصیف شده است.

ب) کاربران باید قادر به درستی‌سنجی اصالت و یکپارچگی توصیه باشند. این موضوع می‌تواند توسط ابزارهای مختلفی شامل امضای رمزنگاری‌شده توصیه انجام شود. پذیرفتن توصیه جعلی و اجرای آن می‌تواند سامانه‌ها را به خطر بیاندازد.

پ) در وضع مطلوب، توصیه و راه‌حل برای آسیب‌پذیری در یک زمان حاضر می‌شود. گرچه شرایط ویژه می‌تواند در زمانی که آسیب‌پذیری به صورت فعال مورد بهره‌برداری قرار می‌گیرد و جزئیات آن منتشر می‌شود، به وجود آید. تحت این شرایط، عرضه‌کننده می‌تواند به جای این که تا زمان تولید راه حل منتظر بماند به کاربران خود با انتشار یک اطلاعیه توصیه یا آگاه‌سازی از طریق راه‌کارهای ممکن (در صورت وجود) خدمت بهتری ارائه کند.

ت) اگر آسیب‌پذیری چندین عرضه‌کننده یا محصول را تحت‌تاثیر قرار دهد، عرضه‌کنندگان باید برای هماهنگ کردن انتشار توصیه که مخاطره را کمینه می‌کند، تلاش کنند.

ث) عرضه‌کنندگان باید ایجاد یک فهرست رایانامه را در نظر گیرند که طرف‌های مدنظر بتوانند مشترک آن شوند. این کار شامل اضافه‌کردن پیوندهای ضروری به وبگاه عرضه‌کننده و خط‌مشی ارسال‌شده خواهد بود.

ج) برای کمک به استفاده‌کنندگان توصیه با ارزیابی تاثیر مرتبط آسیب‌پذیری‌های مختلف، عرضه‌کنندگان باید استفاده از سامانه امتیازدهی شدت آسیب‌پذیری مانند سامانه امتیازدهی آسیب‌پذیری متداول (CVSS) را مورد توجه قرار دهند.

چ) پایگاه داده عمومی که مخزنی مورد اعتماد برای اطلاعات مربوط به آسیب‌پذیری‌های جاری و با جزئیات را نمایش می‌دهد، می‌تواند استفاده شود. این موارد توسط منابع عمومی و خصوصی پیشنهاد می‌شود و در برخی نمونه‌ها می‌تواند مولفه هزینه برای دسترسی به اطلاعات را داشته باشد.

۹-۴ زمانبندی انتشار توصیه

عرضه‌کنندگان باید در زمانبندی انتشار توصیه برای توازن مخاطره کار کنند. در صورتی که آموزشی برای آسیب‌پذیری موجود نباشد اما مهاجمان در حال پیشرفت باشند، عرضه‌کننده ممکن است مجبور به انتشار توصیه برای اطلاع کاربران از مخاطرات و گام‌هایی که آنها می‌توانند برای کمینه کردن و حذف مخاطره انجام دهند، باشد. در غیر این صورت، عرضه‌کنندگان باید توصیه‌هایی را در همان زمانی که آموزش موجود است منتشر کنند. در صورتی که آسیب‌پذیری به صورت فعال توسط مهاجمان مورد بهره‌برداری قرار نمی‌گیرد، مطلوب است تا توصیه و رفع آسیب‌پذیری به سرعت بعد از آماده‌سازی، ارائه شود. گرچه، زمانی که چند توصیه با همان محصول یا خدمت برخط مرتبط است، بهتر است آنها را در همان زمان عرضه کرد تا تعداد وقفه‌های عملیاتی که این رفع آسیب‌پذیری‌های گروهی منجر به آنها خواهد شد، کاهش پیدا کند.

زمانی که آسیب‌پذیری به صورت فعال توسط مهاجمان مورد بهره‌برداری قرار می‌گیرد یا آسیب‌پذیری به صورت عمدی یا غیرعمدی به طور عمومی منتشر می‌شود، عرضه‌کننده مسئول باید به یک توصیه سریع با یک راه‌کار یا رفع آزمایشی را در نظر گیرد. این موضوع ممکن است تا زمانی که وصله یا اصلاحیه ارائه شود، راه‌حلی کوتاه مدت باشد. در این موقعیت، توصیه باید روزآمد شود تا جزئیات فعلی زیر را فراهم آورد:

الف) عرضه‌کنندگان باید در زمان ممکن به هماهنگی انتشار توصیه در نمونه‌هایی که محصولات آن‌ها توسط آسیب‌پذیری‌های مرتبط تحت‌تاثیر قرار گرفته است، تلاش کنند. انتشار اطلاعات در مورد آسیب‌پذیری در یک محصول می‌تواند محصولات وابسته را در معرض مخاطره بیشتری از حمله قرار دهد. این موقعیت به طور معمول زمانی بروز می‌کند که کتابخانه نرم‌افزاری مشترک، پروتکل، پودمان یا سایر مولفه‌ها در چند محصول یا خدمت برخط به کار برده شده باشد. استفاده از هماهنگ‌کننده امکان انتشار کنترل‌شده را می‌دهد و مخاطره برای کاربران را کاهش می‌دهد. زمانی که به جوانب آسیب‌پذیری مربوط به چند عرضه‌کننده توجه می‌شود، آمادگی کارکنان پشتیبانی مشتری در مراکز تماس و قسمت‌های فروش و دیگر جوانب باید مورد توجه قرار گیرد.

ب) دستورکار یابنده برای انتشار

پ) شیوع فعالیت‌هایی که از آسیب‌پذیری بهره‌برداری می‌کند

ت) زمان‌بندی انتشار توصیه سایر عرضه‌کنندگان (زمانی که آسیب‌پذیری چند- عرضه‌کننده وجود داشته باشد)

۹-۵ محتویات توصیه

۹-۵-۱ کلیات

توصیه‌هایی که توسط عرضه‌کنندگان منتشر شده است، باید شامل اطلاعات کافی باشند تا برای جامعه هدف که می‌تواند شامل مدیران سامانه، توسعه‌دهندگان، تصمیم‌گیرندگان، مدیران محصول و غیره باشد، مفید واقع شود. این توصیه‌ها باید به آنها برای تصمیم‌گیری در مورد این که آیا توصیه مربوط به آنها است یا خیر و چگونگی استقرار آموزش یاری رساند.

کاربران توصیه‌ها نیازهای مختلفی دارند که می‌تواند در بخش بازار یا الزامات مقرراتی مستقل باشند. کاربران فنی متخصص مانند یکپارچه‌کننده‌های سامانه به اطلاعات جزئی در مورد تهدیدات و راه‌کارها نیاز دارند. مصرف‌کنندگان به طور معمول برای اطلاعات در خصوص چگونگی تعیین این که آنها در حال استفاده از محصولات تحت‌تاثیر هستند یا خیر ارزش قائل هستند. همچنین این کار زمانی کمک‌کننده است که به زبان ساده باشد و توضیحات قابل درکی برای حل مشکل داشته باشد. توصیه می‌شود که عرضه‌کننده پایه کاربری مورد انتظار را بر اساس ماهیت محصولات آن‌ها تحلیل کند و اطلاعاتی در تمرکز و چیدمان مناسب ارائه کند. مگر این که برخلاف موارد بیان‌شده، ترتیب بخش‌ها نشان از یک عملیات سفارشی نباشد.

بخش‌های زیر، فهرستی از اقلام را با جزئیات بیان می‌کند که باید در توصیه موجود باشد. این فهرست اقلام جامع نیست و عرضه‌کننده می‌تواند بسته به شرایط اطلاعات بیشتر را در توصیه بگنجاند.

۹-۵-۲ شناسانه

شناسانه منحصر به فرد باید برای هر توصیه برای سهولت ارجاع فراهم شود.

۹-۵-۳ عنوان

توصیه می‌شود که عنوان توصیه شامل ارجاع به محصول یا توضیحات دیگری باشد که برای کاربران آگاهی‌دهنده باشد بنابراین خوانندگان توصیه به سرعت می‌توانند تصمیم بگیرند که توصیه به آنها مرتبط است یا خیر.

۹-۵-۴ مرور کلی

بخش مرور کلی گزارش آسیب‌پذیری، خلاصه‌ای سطح بالا از آسیب‌پذیری را فراهم می‌آورد که کاربران می‌توانند نکات برجسته گزارش را درک کنند و به سرعت تعیین کنند که آیا توصیه در محیط آنها کاربردپذیر است یا خیر.

۹-۵-۵ محصولات تحت‌تاثیر

این بخش از توصیه، فهرستی از محصولات تحت‌تاثیر شناخته‌شده و نسخه‌های آنها را ارائه می‌کند. در صورتی که مرتبط باشد، می‌تواند شامل دستورالعمل‌هایی در خصوص چگونگی درستی‌سنجی نسخه محصول در حال استفاده باشد. در اغلب نمونه‌ها، خدمات برخط شناسانه‌های نسخه ندارند اما می‌توانند تاریخ زمانی که آخرین روزآمد/تغییر انجام شده است را داشته باشند.

۹-۵-۶ جامعه هدف

توصیه باید افراد هدف توصیه را از دیدگاه خوانندگان فهرست کند.

۹-۵-۷ شرح

توصیه باید اطلاعات کافی را فراهم آورد تا اگر خوانندگان قانونی تحت‌تاثیر قرار گرفته باشند بتوانند آنها را مستقر کنند و مقدار بهره‌برداری را برآورد کنند. در همین زمان توصیه نباید جزئیات زیادی ارائه کند تا از تسهیل بهره‌برداری از آسیب‌پذیری جلوگیری کند.

۹-۵-۸ تاثیر

توصیه باید اطلاعاتی را فراهم کند که تاثیر آسیب‌پذیری را توصیف کند (برای مثال منع خدمت، اجرای کد). به علاوه سامانه رتبه‌بندی با شدتی (مانند سامانه امتیازدهی آسیب‌پذیری متداول (CVSS)) می‌تواند به منظور ارائه اطلاعات بیشتر برای کمک به کاربران برای ارزشیابی سوءاستفاده از آسیب‌پذیری داده‌شده، استفاده شود.

۹-۵-۹ آموزش

توصیه باید در مورد این که کدام اقدام کاربران برای حل یا کاهش آسیب‌پذیری و تاثیر آن باید انجام شود، اطلاعاتی ارائه دهد. این کار اغلب شامل نصب وصله نرم‌افزاری یا نسخه روزآمدشده برای محصولات نرم‌افزاری است.

تا جایی که مناسب یا ضروری است، توصیه باید راه‌کاری را ارائه کند که کاربران بتوانند محصول یا خدمت برخط تحت‌تاثیر را تا زمانی که راه حل طراحی‌شده پیاده‌سازی می‌شود، محافظت کند. راه‌کارهای معمول شامل تغییر پیکربندی محصول برای محدود کردن کارکرد آن، معرفی دیوار آتش برای محدود کردن دستیابی شبکه برای نمونه محصول و این موارد است.

۹-۵-۱۰ مراجع

مراجع به اطلاعات بیشتر یا مرتبط می‌تواند در این بخش اضافه شوند. مثال‌هایی از این مراجع می‌تواند به توصیه‌های مرتبط که توسط طرف‌های دیگر منتشر شده است یا مرجع به شناسانه آسیب‌پذیری‌ها و رخنه‌پذیری‌های متداول (CVE ID) پیوند داده شود.

۹-۵-۱۱ اعتبار

در این بخش، عرضه‌کننده می‌تواند یابنده را برای گزارش‌دهی آسیب‌پذیری و همکاری در حین فرآیند با فراهم کردن خواسته یابنده برای اعتبار عمومی تصدیق کند.

۹-۵-۱۲ تاریخچه بازنگری

این بخش باید شامل تاریخی باشد که توصیه برای اولین بار انتشار یافته است. در صورتی که توصیه به صورت متعاقب روزآمد می‌شود، این بخش می‌تواند شامل یک تاریخچه اصلاح نیز باشد.

۹-۵-۱۳ اطلاعات تماس

توصیه باید اطلاعات تماس را ارائه دهد تا خوانندگان توصیه بتوانند با عرضه‌کننده تماس بگیرند.

۹-۵-۱۴ مدت استفاده

توصیه باید اطلاعاتی را در مورد حق نشر و شرایط استفاده و توزیع مجدد توصیه ارائه کند.

۹-۶ ارتباط توصیه

عرضه‌کنندگان باید روش‌های مناسبی را برای ارتباط توصیه‌ها با کاربران خود ایجاد و نگهداری کنند. روش‌های معمول شامل وبگاه‌ها، فهرست‌های رایانامه، خوراک‌ها[1]، سازوکارهای روزآمد خودکار است. هر عرضه‌کننده می‌تواند بهترین روش را برای استفاده در جامعه کاربری خود تعیین کند. عرضه‌کنندگان می‌توانند همچنین انتخاب کنند تا توصیه‌ها را به انجمن‌های بحث عمومی آسیب‌پذیری ارسال کنند تا اطلاعات خود را با جامعه بزرگتری به اشتراک بگذارند.

۹-۷ قالب‌های توصیه

قالب ثابت برای توصیه‌ها باید حفظ شود تا سطح درک توصیه افزایش یابد. در حالی که تغییرات برای قالب باید در زمان موردنیاز انجام شود، این تغییرات نباید با فواصل زمانی کم انجام شود تا کاربران بتوانند برخی از فرآیندها را در خصوص ویژگی‌های مهم توصیه سفارشی کنند.

در زمان ایجاد توصیه، تولیدکنندگان توصیه باید به فراهم کردن محتوا در هر دو قالب قابل خواندن برای انسان و ماشین توجه کنند. مثال‌هایی از توصیه‌های قابل خواندن برای انسان در بند ب-۳ فراهم آمده است.

۹-۸ اصالت توصیه

کاربران باید قادر به درستی‌سنجی اصالت توصیه باشند. این کار ممکن است توسط امضای رمزنگاری‌شده توصیه انجام شود. پذیرش توصیه جعلی و اجرای آن می‌تواند باعث به خطر انداختن سامانه‌ها شود.

بسته به فن رمزنگاری استفاده‌شده، عرضه‌کننده باید اقلام رمزنگاری‌شده موردنیاز و اعتبارنامه‌ها[2] را در وبگاه منتشر کند (مانند کلیدهای عمومی یا گواهینامه‌ها).

1 - Feeds
2 - Credentials

پیوست الف
(اطلاعاتی)
جزییات برای ساماندهی آسیب‌پذیری/ اطلاعات توصیه

به منظور کمک به عرضه‌کننده در ساماندهی گزارش آسیب‌پذیری، عرضه‌کننده می‌تواند درخواست کند که یابنده اطلاعات با جزئیات زیر را ارائه دهد. عرضه‌کننده می‌تواند برای ارائه این اطلاعات، وبگاه یا سایر ابزارهای الکترونیکی را پیشنهاد کند.

اطلاعات مورد نیاز بر اساس راه‌حل عرضه‌کننده و درخواست/ خدمت تحت‌تاثیر، متفاوت خواهد بود.

اطلاعات زیر در هنگام ارائه گزارش به عرضه‌کننده مفید خواهد بود.

الف-۱ محصول

الف-۱-۱ مبتنی بر COTS

الف) نام محصول - نام متداول مورد استفاده برای راه‌حل.

ب) سامانه عامل - سامانه عامل نصب‌شده.

پ) شماره نسخه با استفاده از نامگذاری عرضه‌کننده در صورت امکان - شماره نسخه در صورت امکان شامل جزئیات کلی و جزئی محصول منتشر شده است.

ت) شرح فنی - ارائه این که چه اقداماتی انجام شده است و نتیجه تا حد ممکن با جزئیات.

ث) کد نمونه - در صورت امکان، ارائه کدی که برای ایجاد آسیب‌پذیری در آزمایش استفاده شده است.

ج) اطلاعات تماس یابنده - بهترین روش برای رسیدن به یابنده.

چ) سایر طرف‌هایی که با موضوع سروکار دارند – در صورت وجود طرف‌های دیگر.

ح) طرح(های) افشا - طرح کنونی برای افشا.

خ) ارزیابی تهدید / مخاطره - شامل جزییات مربوط به تهدیدات شناسایی‌شده و / یا مخاطرات شامل سطح مخاطره (بالا، متوسط، پایین) برای نتیجه ارزیابی.

د) پیکربندی نرم‌افزار - جزئیات پیکربندی رایانه / افزاره در زمان آسیب‌پذیری.

ذ) اطلاعات مربوط به افزاره‌های متصل اگر آسیب‌پذیری در طول تعامل به وجود آید. هنگامی که افزاره ثانویه باعث آسیب‌پذیری می‌شود، این جزئیات باید ارائه شود.

الف-۱-۲ مبتنی بر سخت‌افزار

الف) مدل سخت‌افزار در صورت امکان با استفاده از نامگذاری عرضه‌کننده.

ب) تعداد ویرایش‌های سخت‌افزار - می‌تواند از واسط خط فرمان یا سایر واسط‌های مدیریتی به دست آید.

پ) شرح فنی - ارائه این که چه اقداماتی انجام شده است و نتیجه تا حد ممکن با جزئیات.

ت) کد نمونه - در صورت امکان، ارائه کدی که برای ایجاد آسیب‌پذیری در آزمایش استفاده شده است.

ث) اطلاعات تماس یابنده - بهترین روش برای رسیدن به یابنده.

ج) سایر طرف‌هایی که با موضوع سروکار دارند – در صورت وجود طرف‌های دیگر.

چ) طرح(های) افشا - طرح کنونی برای افشا.

ح) ارزیابی تهدید/ مخاطره - شامل جزییات مربوط به تهدیدات شناسایی‌شده/ یا مخاطرات شامل سطح مخاطره (بالا، متوسط، پایین) برای نتیجه ارزیابی.

خ) پیکربندی نرم‌افزار - جزئیات پیکربندی رایانه/ افزاره در زمان آسیب‌پذیری.

د) اطلاعات مربوط به افزاره‌های متصل اگر آسیب‌پذیری در طول تعامل به وجود آید. هنگامی که افزاره ثانویه باعث آسیب‌پذیری می‌شود، این جزئیات باید ارائه شود.

الف-۱-۳ مبتنی بر ابر[1]

الف) برای آسیب‌پذیری‌های خدمات برخط، زمان و تاریخ کشف؛

ب) برای آسیب‌پذیری‌های خدمات برخط، URL؛

پ) برای آسیب‌پذیری‌های خدمت برخط، اطلاعات مرورگر شامل نوع و نسخه.؛

ت) برای آسیب‌پذیری‌های خدمت برخط، ورودی مورد نیاز برای تولید مجدد آسیب‌پذیری؛

ث) شرح فنی - ارائه این که چه اقداماتی انجام شده است و نتیجه تا حد ممکن با جزئیات؛

ت) کد نمونه - در صورت امکان، ارائه کدی که برای ایجاد آسیب‌پذیری در آزمایش استفاده شده است؛

ث) اطلاعات تماس یابنده - بهترین روش برای رسیدن به یابنده؛

ج) سایر طرف‌هایی که با موضوع سروکار دارند – در صورت وجود طرف‌های دیگر؛

چ) طرح(های) افشا - طرح کنونی برای افشا؛

ح) ارزیابی تهدید/ مخاطره - شامل جزییات مربوط به تهدیدات شناسایی‌شده و/ یا مخاطرات شامل سطح مخاطره (بالا، متوسط، کم) برای نتیجه ارزیابی؛

خ) پیکربندی نرم‌افزار - جزئیات پیکربندی رایانه/ افزاره در زمان آسیب‌پذیری؛

د) اطلاعات مربوط به افزاره‌های متصل اگر آسیب‌پذیری در طول تعامل به وجود آید. هنگامی که افزاره ثانویه باعث آسیب‌پذیری می‌شود، این جزئیات باید ارائه شود.

1 – Cloud based

الف-۲ فرم گزارش آسیب‌پذیری

در صورت امکان، برای کسب اطلاعات لازم باید از فرم گزارش آسیب‌پذیری استفاده شود. موارد زیر مثال‌هایی از CERT /CC و JPCERT هستند.

الف-۲-۱ فرم گزارش آسیب‌پذیری CERT/CC

فرم گزارش آسیب‌پذیری

ما گزارش‌های آسیب‌پذیری‌های امنیتی را می‌پذیریم و به عنوان یک نهاد هماهنگی که با عرضه‌کنندگان تحت‌تاثیر کار می‌کند، برای رفع آسیب‌پذیری به ارائه خدمت می‌پردازیم. اگر بر این باور هستید، یک آسیب‌پذیری امنیتی که حل نشده است را یافته‌اید، لطفا فرم زیر را پر کنید. همان طور که خط‌مشی افشای آسیب‌پذیری ما توضیح می‌دهد، ما اطلاعات ارائه‌شده در گزارش آسیب‌پذیری را به عرضه‌کنندگان تحت‌تاثیر ارسال می‌کنیم. به طور پیش‌فرض، ما نام شما را با عرضه‌کنندگان به اشتراک خواهیم گذاشت و در مستنداتی که منتشر می‌کنیم به صورت عمومی از شما قدردانی خواهیم کرد. اگر شما بخواهید نامتان به اشتراک گذاشته نشود یا به صورت عمومی از شما قدردانی نشود، یکی از پاسخ‌های مناسب زیر انتخاب کنید.

برای کسب اطلاعات بیشتر درباره فیلدهای این فرم، به دستورالعمل مراجعه کنید. در صورت وجود هرگونه مشکل یا در صورتی که می‌خواهید از قالب دیگری برای ارائه این گزارش استفاده کنید، با ما تماس بگیرید.

لطفا تا آنجا که می‌توانید اطلاعات ارائه دهید. پس از اتمام، گزارش خود را با استفاده از دکمه‌ای که در انتهای فرم قرار دارد، ارسال کنید.

اطلاعات تماس شما

اطلاعات تماس خود را صورت داشتن سوالات افزوده ما در مورد این گزارش آسیب‌پذیری، ارائه دهید. این اطلاعات برای گزارش آسیب‌پذیری مورد نیاز نیست، اما بدون آن، ما قادر به تماس با شما نخواهیم بود.

نام:

سازمان:

رایانامه:

تلفن:

آیا می‌توانیم نام شما را به عرضه‌کننده ارائه دهیم؟ بله خیر

آیا می‌خواهید به صورت عمومی از شما قدردانی شود؟ بله خیر

شرح آسیب‌پذیری

لطفا آسیب‌پذیری را شرح دهید.

پر کردن این فیلد الزامی است.

بر این باورید که کدام یک از پیکربندی‌های سامانه آسیب‌پذیر هستند؟

اگر بر این باورید که از آسیب‌پذیری بهره‌برداری شده است، اینجا را علامت بزنید.

اگر این بهره‌برداری در دسترس عموم است، اینجا را علامت بزنید.

تاثیر بهره‌برداری از این آسیب‌پذیری

تاثیرات خاص را شرح دهید و این که تصور می‌کنید چگونه این آسیب‌پذیری در یک سناریوی (فرانامه‌ی)[1] حمله استفاده می‌شود:

اطلاعات تماس عرضه‌کننده

کدام یک از عبارات زیر، بهترین توصیف ارتباط شما با عرضه‌کننده یا عرضه‌کنندگان است؟

من به عرضه‌کننده اطلاع نداده‌ام و قصد این کار را هم ندارم.

من به عرضه‌کننده اطلاع نداده‌ام، اما قصد این کار را دارم.

من در حال حاضر به عرضه‌کننده اطلاع داده‌ام.

من نماینده عرضه‌کننده محصول آسیب‌پذیر هستم.

عرضه‌کننده در حال حاضر به صورت عمومی آسیب‌پذیری را تایید کرده است.

عرضه‌کننده محصولی که شامل آسیب‌پذیری است، چه کسی است؟ اگر شما در حال حاضر در رابطه با این مشکل با عرضه‌کننده تماس حاصل کرده‌اید، لطفا اطلاعات تماس و هرگونه شماره پیگیری را با ما به اشتراک بگذارید. اگر عرضه‌کنندگان متعددی تحت‌تاثیر قرار می‌گیرند، آنها را فهرست کنید و در اطلاعات افزوده عرضه‌کننده توضیح دهید که چگونه آنها تحت‌تاثیر قرار می‌گیرند.

نام عرضه‌کننده:

نام تماس:

رایانامه تماس:

تلفن تماس:

شماره پیگیری عرضه‌کننده:

اطلاعات افزوده *عرضه‌کننده*

هرگونه اطلاعات افزوده درباره عرضه‌کننده و ارتباطات شما با آنها را ارائه دهید.

بارگذاری پرونده

1 - Senario

شما می‌توانید یک (۱) پرونده مرتبط را برای ارسال به ما مشخص کنید:

شماره‌های پیگیری CERT

اگر شما یک یا چند شماره پیگیری CERT برای این گزارش دارید، آنها را در اینجا وارد کنید:

نظرات افزوده

شما می‌توانید هرگونه نظرات دیگری که می‌خواهید شامل شود را ارائه دهید:

ارسال گزارش

با تشکر از وقتی که برای تکمیل فرم گزارش آسیب‌پذیری صرف کردید. برای ارسال گزارش خود بر روی دکمه زیر کلیک کنید.

الف-۲-۲ فرم گزارش آسیب‌پذیری نمایندگی توسعه فناوری اطلاعات (IPA)[1] و مرکز هماهنگی تیم پاسخ اضطراری رایانه‌ای ژاپن (JPCERT)[2]

الف) توافق‌نامه خط‌مشی ساماندهی آسیب‌پذیری

می‌پذیرم (گزارشگر موافقت می‌کند) که IPA و JPCERT/CC اطلاعات آسیب‌پذیری گزارش‌شده را مطابق با راهنمای ساماندهی اطلاعات مربوط به آسیب‌پذیری که در وبگاه IPA اعلام شده است، نگهداری و پردازش کند.

(اگر چنین نیست، IPA نمی‌تواند گزارش‌آسیب‌پذیری را دریافت و ساماندهی کند.)

ب) اطلاعات تماس یابنده

۱) اطلاعات تماس

نشانی (با دقت در سطح استان به جای آدرس کامل):

وابستگی:

نام (نام کامل یا نام مستعار):

رایانامه:

شماره تلفن:

شماره نمابر:

در صورتی که یکی از موارد رایانامه، شماره تلفن، شماره نمابر در دسترس باشد، سایر موارد غیر از «نام» اختیاری است.

1 - INFORMATION-TECHNOLOGY PROMOTION AGENCY
2 - Japan Computer Emergency Response Team Coordination Center

۲) استفاده قابل قبول از اطلاعات گزارشگر، یکی از موارد زیر را انتخاب کنید.

أ) گزارشگر موافقت می‌کند که IPA می‌تواند اطلاعات تماس گزارشگر را به JPCERT/CC و عرضه‌کننده محصول ارسال کند.

ب) گزارشگر از IPA می‌خواهد اطلاعات تماس گزارشگر را مخفی نگه دارد و به عنوان یک پیشکار[1] در ارتباط احتمالی با JPCERT/CC و عرضه‌کننده محصول عمل کند.

ج) برای قدردانی از توصیه به گزارشگر مراجعه کند.

I) در توصیه‌های JPCERT/CC، یکی از موارد زیر را انتخاب کنید:

الف. نام گزارشگر و/ یا وابستگی می‌تواند شامل شود؛

ب. نام گزارشگر و/ یا وابستگی نباید اظهار شود.

II) در توصیه‌های عرضه‌کنندگان محصول، یکی از موارد را انتخاب کنید:

الف. نام گزارشگر و/ یا نام وابستگی می‌تواند شامل شود؛

ب. نام گزارشگر و/ یا نام وابستگی نباید اظهار شود.

اگر نام گزارشگر بتواند در توصیه‌ها شامل شود، لطفا مشخص کنید که چگونه باید به آن ارجاع شود:

وابستگی گزارشگر به زبان کشور:

وابستگی گزارشگر به زبان انگلیسی:

نام گزارشگر به زبان کشور:

نام گزارشگر به زبان انگلیسی:

پ) اطلاعات مربوط به آسیب‌پذیری

۱) منبع اطلاعات، یکی از موارد زیر را انتخاب کنید:

أ) خود گزارشگر.

ب) یکی از آشنایان گزارشگر.

ج) BBS، وبلاگ، و غیره (URL)[2].

۲) محصولی که در آن آسیب‌پذیری پیدا شده است.

أ) نام محصول:

1 - Proxy
2 - Uniform Resource Location

ب) نسخه نرم‌افزار:

ج) وصله و اصلاحیه:

د) نسخه زبان:

ه) انحراف از پیکربندی استاندارد:

و) نام عرضه‌کننده محصول:

ز) نشانی وب (URL) عرضه‌کننده محصول:

اطلاعات در مورد نسخه جزئی، وصله‌های نصب‌شده، بسته خدمت (سرویس پک)[1] و هاتفیکس باید در «وصله و اصلاحیه» شامل شود.

۳) رفتار غیر عادی ناشی از آسیب‌پذیری

۴) روال تولید مجدد وضعیت آسیب‌پذیر

۵) احتمال تولید مجدد، یکی از موارد زیر را انتخاب کنید:

أ) همیشه

ب) اغلب

ج) به ندرت

نظرات افزوده برای تولید مجدد وضعیت (مانند وابستگی به نسخه، زبان و غیره).

۶) تهدید احتمالی ناشی از آسیب‌پذیری

۷) راه‌کار

۸) کد اثبات مفهوم (PoC)

۹) سایر نظرات از گزارشگر (شامل ارزیابی شدت)

ت) در دسترس بودن جهانی محصول، یکی از پنج مورد زیر را انتخاب کنید:

۱) نرم‌افزار در خارج کشور توسعه داده شده است.

۲) نرم‌افزار در داخل کشور توسعه داده شده و برخی محصولات شامل آن به طور گسترده در کشورهای خارجی توزیع شده است.

۳) نرم‌افزار در داخل کشور توسعه داده شده و همچنین در کشورهای خارجی توزیع شده است.

1 - Service pack

۴) نرم‌افزار در داخل کشور توسعه داده شده و گزارشگر نمی‌داند که آیا در کشورهای خارجی توزیع شده است یا نه.

۵) سایر ( )

ث) آیا شما (گزارشگر) در حال حاضر آسیب‌پذیری را به طرف‌های دیگر به غیر از IPA گزارش داده‌اید؟ یکی از دو مورد زیر را انتخاب کنید:

۱) بله، گزارش داده‌ام.

- تاریخ گزارش:

- شناسانه گزارش:

- نام طرف:

- نام شخصی که با آن تماس حاصل کرده‌اید:

- رایانامه تماس او:

- شماره تلفن تماس او:

۲) نه، گزارش نداده‌ام.

ج) پروتکل برای ارتباط بیشتر. آیا شما (گزارشگر) می‌خواهید پیام‌هایی که از IPA ارسال می‌شود، رمزگذاری شود؟

یکی از موارد زیر را انتخاب کنید:

بله

خیر

در این صورت، لطفا کلید عمومی را ضمیمه کنید.

ح) موارد دیگری که باید گزارش شود.

الف-۳ محتوای یک توصیه

علاوه بر فهرست توصیه ارائه‌شده در بند ۹-۵، این بند فهرست جامع‌تری از فیلدهایی که می‌تواند در توصیه گنجانده شود را ارائه می‌کند.

مرورکلی

این توصیه باید ابتدا خلاصه‌ای از آسیب‌پذیری را ارائه کند که کاربران بتوانند به سرعت نکات اساسی را درک کنند.

نرم‌افزار آسیب‌پذیر

در صورت امکان، توصیه باید فهرستی توصیفی از محصولات و نسخه‌های تحت‌تاثیر را ارائه کند. همچنین ممکن است شامل توضیحی از نحوه تایید نسخه این محصولات شامل قرارداد نامگذاری عرضه‌کننده برای نامگذاری و شماره‌دهی باشد.

شناسانه منحصر به فرد

در هنگام مواجهه با اطلاعات آسیب‌پذیری، نام‌ها می‌تواند گیج‌کننده باشد. در برخی موارد، می‌تواند منجر به تفسیر آسیب‌پذیری نادرست و به طور بالقوه سبب به مخاطره افتادن سامانه شود. بنابراین، ضروری است که توصیه از هر دو شماره منحصر به فرد و قرارداد نامگذاری استفاده کند. سامانه فعلی که توسط بسیاری از منابع استفاده می‌شود شامل MTRE /CVE است که از قالب‌های زیر استفاده می‌کند:

CVE-YYYY- #### که در آن 'Y' نشان‌دهنده سال افشا است.

این سامانه شامل طرحی بین‌المللی است که می‌تواند برای پیدا کردن شماره یک آسیب‌پذیری خاص به آن ارجاع شود. این امر، این حقیقت که یک مولفه ممکن است دارای قرارداد نام‌گذاری و شماره‌دهی خود باشد یا نباشد را مستثنی نمی‌کند. این امر اجازه می‌دهد مالک مولفه و طرف‌های موردنظر، جزئیات خاصی از آسیب‌پذیری را تعیین کنند و تضمین می‌کند که تفسیر نادرست بالقوه کمینه شود.

در حال حاضر چندین روش برای تبادل اطلاعات آسیب‌پذیری وجود دارد. به طور مثال:

الف) شناسانه منحصر به فرد

۱) شناسانه‌ها و واژه‌نامه آسیب‌پذیری‌ها و رخنه‌پذیری‌های متداول (CVE) برای آسیب‌پذیری‌های امنیتی مربوط به نقص‌های نرم‌افزاری؛

۲) شناسانه‌ها و واژه‌نامه شمارش پیکربندی متداول (CCE)[1] برای مسائل پیکربندی سامانه که مربوط به امنیت است؛

۳) شناسانه‌ها و واژه‌نامه شمارش بستر متداول (CPE)[2] برای نامگذاری بستر/ محصول؛

ب) سامانه‌های امتیازدهی

۱) سامانه امتیازدهی آسیب‌پذیری متداول (CVSS)[3].

این روش‌ها تا حد زیادی می‌تواند در افزایش دسترسی به اطلاعات افشاشده به تمام طرف‌های ذینفع کمک کند و باید توسط عرضه‌کنندگان هنگام انتشار افشا در نظر گرفته شود.

1 - Common Configuration Enumeration
2 - Common Platform Enumeration
3 - Common Vulnerability Scoring System

به منظور ترویج تبادل اطلاعات خودکار و ارائه سازگاری اطلاعات بیشتر در میان عرضه‌کنندگان، عرضه‌کنندگان باید اطلاعات آسیب‌پذیری و رخنه‌پذیری‌های متداول (CVE) و سامانه امتیازدهی آسیب‌پذیری متداول (CVSS) را به عنوان بخشی از توصیه های خود در نظر گیرند. هر دوی این موارد، بخشی از توصیه‌نامه ITU-T X.1500 [1] است (Cybex).

در اغلب موارد، CVE پیشگام، به طور مستقیم، شماره‌های شناسانه-CVE را صادر نمی‌کند اما در عوض متکی به سازوکارهای خاصی برای ساماندهی اطلاعات در حال ظهور تازه است که در نهایت به CVE ارائه می‌شود. بنابراین، برای دریافت شماره CVE-ID، عرضه‌کننده باید یکی از موارد زیر را انجام دهد:

الف) تماس با یکی از مراجع ذیصلاح شماره‌گذاری CVE (CNAs)[2] فهرست‌شده در پیوند[3] زیر که پس از آن شماره CVE-ID در اطلاعیه عمومی اولیه خود درباره آسیب‌پذیری جدید شما شامل خواهد شد؛

ب) تماس با تیم پاسخ اضطراری مانند CERT/CC، قابلیت توصیه رخداد رایانه‌ای در اداره انرژی (DOE-CIAC)[4]، اولین تیم پاسخ اضطراری رایانه‌ای ملی کانادا (CanCERT)[5]، و غیره؛

پ) ارائه اطلاعات به تیم تحلیل آسیب‌پذیری؛

ت) ارائه CVE یا دیگر شماره تخصیص‌یافته به یابنده؛

فهرستی از مراجع شماره‌گذاری CVE در http://cve.mitre.org/cve/cna.html موجود است.

آسیب‌پذیری‌ها و رخنه‌پذیری متداول (توصیه‌نامه ITU-T X.1520)، فهرستی از آسیب‌پذیری‌ها و رخنه‌پذیری‌های امنیت اطلاعات است که هدف آن ارائه نام‌های متداول برای مشکلات شناخته‌شده عمومی است. هدف از CVE آسان‌تر کردن اشتراک داده‌ها در میان قابلیت‌های آسیب‌پذیری جداگانه (ابزارها، مخازن و خدمات) با این «شمارش متداول» است. قصد CVE جامع شدن با توجه به تمام آسیب‌پذیری‌ها و رخنه‌پذیری‌های عمومی است. با استناد به CVE در توصیه، کاربران راحت‌تر می‌توانند تشخیص دهند که کدام آسیب‌پذیری موضوع توصیه است. اطلاعات بیشتر در مورد CVE در آدرس http://cve.mitre.org موجود است.

سامانه امتیازدهی آسیب‌پذیری متداول (توصیه‌نامه ITU-T X.1521) برای چارچوب باز برقراری ارتباط، مشخصه‌ها و تاثیرات آسیب‌پذیری‌های IT را ارائه می‌کند. CVSS شامل سه گروه است: پایه، زمانی و محیطی. هر گروه امتیاز عددی در محدوده ۰ تا ۱۰ و یک بردار نمایش متنی فشرده که منعکس‌کننده مقادیر استفاده‌شده برای استخراج امتیاز است را تولید می‌کند. گروه پایه نشان‌دهنده کیفیت‌های ذاتی آسیب‌پذیری است. گروه زمانی، منعکس‌کننده مشخصه‌های آسیب‌پذیری است که در طول زمان تغییر می‌کند. گروه محیطی، ارائه‌دهنده مشخصه‌های آسیب‌پذیری است که منحصر به محیط هر کاربر است.

1 - The ITU Telecommunication Standardization Sector
2 - CVE Numbering Authorities
3 - link
4 - Computer Incident Advisory Capability at the Department of Energy
5 - Canada's first national Computer Emergency Response Team

CVSS تمام مدیران IT، ارائه‌دهندگان خبرنامه آسیب‌پذیری، عرضه‌کنندگان امنیتی، عرضه‌کنندگان برنامه‌های کاربردی و محققان را قادر می‌سازد تا با اتخاذ یک زبان مشترک امتیازدهی آسیب‌پذیری‌های IT از منافع آن بهره ببرند. اطلاعات بیشتر در مورد CVSS در http://www.first.org/cvss قابل دسترسی است.

شرح

برای اطمینان از این که کاربران آسیب‌پذیری را با سایر آسیب‌پذیری‌های مشخص‌شده در همان محصول اشتباه نمی‌گیرند، توصیه باید آسیب‌پذیری را به وضوح با مشخص کردن نام، علت و سایر اطلاعات در دسترس، توضیح دهد.

تهدیدات

توصیه باید اطلاعات در مورد تهدیدات شناخته‌شده که به آسیب‌پذیری مربوط است را ارائه دهد (به طور مثال وجود بهره‌برداری یا کد اثبات مفهوم، بحث یا مدرکی دال بر فعالیت حادثه).

اثر

توصیه باید پیامدهای بالقوه/ مورد انتظار حملات در برابر آسیب‌پذیری را شرح دهد. حملات می‌تواند اثرات متعددی داشته باشد (به طور مثال حمله در برابر آسیب‌پذیری سرریز بافر می‌تواند باعث ازکارافتادگی[1] یا اجرای کد شود). در صورت امکان، اثرات ثانویه شرح داده شود (به طور مثال آسیب‌پذیری نبشته سایت قلابی به طور مستقیم اجازه تزریق محتوا به صفحه وب را به مهاجم می‌دهد. با این حال، اثر ثانویه می‌تواند رخنه‌پذیری کوکی‌ها یا سایر اعتبارنامه‌های اصالت‌سنجی باشد).

راه‌حل

برای آسیب‌پذیری‌های محصول، توصیه باید اطلاعات در مورد نحوه نصب محصول اصلاح شده، روزآمد و اعمال وصله‌های اصلاحیه امنیتی محصول را ارائه دهد.

راه‌کارها

در صورتی که کاربران بتوانند بدون اعمال وصله‌های امنیتی، محصولات تحت تاثیر در حال استفاده را از طریق تلاش‌های عملیاتی یا تا حدی با محدودکردن استفاده از آن، محافظت کنند، توصیه باید اطلاعات راه‌کار را ارائه دهد.

منابع

اگر اطلاعات بیشتری در مورد آسیب‌پذیری که کاربران می‌توانند به آن مراجعه کنند در دسترس باشد، توصیه باید پیوندهایی را به عنوان مرجع ارائه دهد.

1 - Crash

اعتبار

برخی از عرضه‌کنندگان نرم‌افزار به عامل کشف و گزارش‌های آسیب‌پذیری اعتبار ارائه می‌کنند. بسته به خط‌مشی/ شیوه عرضه‌کننده صادرکننده توصیه باید اعتبار مناسبی ارائه شود.

تاریخچه بازبینی‌ها

توصیه باید تاریخی که در آن آسیب‌پذیری رخ داده و آن چه به‌روزشده را روشن کند.

اطلاعات تماس

در مواقعی که اطلاعات آسیب‌پذیری، نامشخص است یا وصله‌های امنیتی باعث برخی مسائل شده، توصیه باید اطلاعات تماس را ارائه دهد.. در صورت امکان، بازبینی نرم‌افزار، شناسانه وصله، شماره اصلاحیه، تاریخ و غیره باید برای اطمینان از این که نرم‌افزار خاص به درستی به کاربر نهایی شناخته شده است، دربرگرفته شود.

پیوست ب
(اطلاعاتی)
خط‌مشی‌های نمونه، توصیه‌ها و هماهنگ‌کننده‌های جهانی

ب-۱ خط‌مشی افشای آسیب‌پذیری نمونه

خط‌مشی زیر می‌تواند به عنوان نمونه استفاده شود یا خط‌مشی‌ای بر طبق آن ایجاد شود. این خط‌مشی می‌تواند به عرضه‌کنندگان نرم‌افزار و مبتنی بر خدمات اعمال شود. خط‌مشی‌ها و بیانیه‌های زیر راهنمای حقوقی را منعکس نمی‌کند و توصیه می‌شود که هر شرکتی که خط‌مشی‌ای را ارسال می‌کند توصیه‌های حقوقی را به منظور تعیین مناسب و هم‌سو با قوانین و قوانین محلی جستجو کند.

مقدمه

<نام شرکت>[1] متعهد به حل آسیب‌پذیری‌ها به منظور برآورده ساختن نیازهای مشتریان و جامعه فناوری گسترده‌تر می‌شود.

این مستند، خط‌مشی <نام شرکت> برای دریافت گزارش‌های مربوط به آسیب‌پذیری‌های امنیتی بالقوه در محصولات و خدمات خود و روش استاندارد شرکت با توجه به اطلاع‌رسانی به مشتریان از آسیب‌پذیری‌های درستی‌سنجی‌شده را توصیف می‌کند.

زمان تماس با تیم پاسخ اضطراری امنیتی

در شرایط زیر با تیم پاسخ اضطراری امنیت رایانه‌ای (CSERT)[2] <نام شرکت> با ارسال ایمیل به security-alert@<company domain name> تماس حاصل کنید:

- یک آسیب‌پذیری امنیتی بالقوه در یکی از محصولات ما شناسایی کرده‌اید.

- یک آسیب‌پذیری امنیتی بالقوه در یکی از خدمات ما شناسایی کرده‌اید.

پس از دریافت گزارش رخداد شما، کارکنان مناسب برای پیگیری با شما تماس خواهند گرفت.

برای اطمینان از محرمانگی، ما شما را به رمزگذاری هرگونه اطلاعات حساسی که به ما از طریق رایانامه ارسال می‌کنید، تشویق می‌کنیم. ما مجهز به دریافت پیام‌های رمزگذاری‌شده با استفاده از S/MIME هستیم. رونوشتی از گواهی که می‌تواند برای ارسال رایانامه‌های رمزگذاری‌شده استفاده شود در وبگاه ما در مورد این خط‌مشی یافت می‌شود.

نشانی رایانامه security-alert@<company domain name> **فقط** به منظور گزارش‌دهی آسیب‌پذیری‌های امنیتی محصول یا خدمات در نظر گرفته شده است و برای اطلاعات پشتیبانی فنی در مورد محصولات یا خدمات ما نیست. تمامی مطالب غیر از مطالبی که خاص آسیب‌پذیری‌های امنیتی در محصولات یا خدمات

۱- نام شرکت یا سازمان جایگزین این قسمت می‌شود.

2 - Computer Security Emergency Response Team

ما است، حذف خواهد شد. برای سوالات فنی و پشتیبانی مشتریان، لطفا <پیوند وبگاه شرکت بـه پشـتیبانی فنی > را ملاحظه فرمایید.

<نام شرکت> تلاش به تایید دریافت تمام گزارش‌های ارسال‌شده ظرف مدت هفت روز را دارد.

دریافت فرم اطلاعات امنیتی از <نام شرکت>

اطلاعات امنیتی فنی در مورد محصولات و خدمات ما از طریق چندین کانال توزیع می‌شود.

الف) <نام شرکت> اطلاعات در مورد آسیب‌پذیری‌های امنیتی را به مشتریان از طریـق رایانامـه بـه <نـام و پیوند به نشانی‌هایی استفاده‌شده برای تماس> توزیع می‌کند. در اغلب موارد، ما هنگام شناسایی راه‌کارهـای عملی یا رفع آسیب‌پذیری‌های امنیتی خاص اطلاعیه‌ای را صادر خواهیم کرد، هر چند در برخی موارد ممکن است در صورتی که آسیب‌پذیری به طور گسترده‌ای در جامعه امنیتی شناخته شده باشد حتی در صورتی که راه‌کاری وجود نداشته باشد نیز اطلاعیه‌ای را صادر کنیم.

از آنجا که هر مورد آسیب‌پذیری امنیتی متفاوت است، می‌توانیم در ارتباط بـا صـدور اعلامیـه‌هـای امنیتـی اقدامات جایگزین را به کار گیریم. <نام شرکت> می‌تواند به انتشار اعلامیه سرعت ببخشد یا آن را به تـاخیر اندازد یا اطلاعیه را هرگز صادر نکند. <نام شرکت> تضمین نمی‌کند که اعلامیه‌های امنیتی برای هر یا همه موضوعات امنیتی که مشتریان قابل توجه در نظر می‌گیرند صادر شود یا که آن اعلامیه‌ها در هر جدول زمانی خاص صادر شود.

ب) اطلاعات مربوط به امنیت نیز می‌تواند توسط <نام شرکت> به گروه‌های خبری عمومی یا فهرسـت‌هـای رایانامه توزیع شود. این موضوع به صورت اقتضایی بسته به نحوه درک <نام شرکت> از ارتباط هر اعلامیه به هر انجمن خاص، انجام می‌شود.

پ) <نام شرکت> با جامعه پاسخ رخداد رسمی برای توزیع اطلاعات کار مـی‌کنـد. بسـیاری از اعلامیـه‌هـای امنیتی شرکت توسط CSERT منطقه‌ای در همان زمان که از طریق کانال‌های توزیع اطلاعات شرکت ارسال می‌شود، توزیع می‌شود.

تمام جنبه‌های این فرآیند ممکن است بدون اطلاع قبلی و به صورت استثنا مورد به مورد تغییـر کنـد. هـیچ سطح خاصی از پاسخ برای هر موضوع خاص یا طبقه‌ای از مسائل تضمین نمی‌شود.

سلب مسئولیت:

استفاده از اطلاعات به منزله قبول استفاده در شرایط AS IS[1] است. هیچ بیانیـه یـا ضـمانت‌نامـه ضمنی یا تضمینی با توجه به این اطلاعات وجود ندارد. نویسنده و ناشر هـیچ‌گونـه مسـئولیتی را برای از دست دادن مستقیم، غیرمستقیم یا زیان مهم یا آسیب ناشی از استفاده یا تکیه بـر ایـن اطلاعات قبول نمی‌کند.

۱- AS IS، به عنوان یک اصطلاح قانونی استفاده می‌شود تا برخی ضمانت‌های ضمنی برای یک قلم فروخته شده را انکار کند.

ب-۲ نمونه‌های توصیه

در زیر برخی توصیه‌های نمونه ارائه شده است. این توصیه‌ها باید به عنوان مدلی از محتوای خوب و جزئیات برای ارائه به کاربران ارجاع داده شود. توصیه‌های بیان‌شده در اینجا تنها یک خلاصه است. توصیه می‌شود که پیوندهای ارائه‌شده برای دریافت توصیه کامل به عنوان مرجع مشاهده شود.

ب-۲-۱ مثال توصیه از مایکروسافت

خبرنامه امنیتی مایکروسافت MS09-018 - حیاتی

آسیب‌پذیری اکتیو دایرکتوری[1] اجازه اجرای کد از دور[2] را می‌دهد (۹۷۱۰۵۵)

تاریخ انتشار: ۹ ژوئن سال ۲۰۰۹

ویرایش: ۱.۰

اطلاعات عمومی

خلاصه اجرایی

این روزآمد امنیتی دو آسیب‌پذیری خصوصی گزارش‌شده در پیاده‌سازی اکتیو دایرکتوری در ویندوز کارساز ۲۰۰۰ و ویندوز کارساز ۲۰۰۳ و حالت کاربردی اکتیو دایرکتوری (ADAM)[3] زمانی که بر روی ویندوز XP حرفه‌ای و ویندوز کارساز ۲۰۰۳ نصب می‌شود را حل می‌کند. آسیب‌پذیری شدیدتر می‌تواند اجازه اجرای کد از دور را دهد. مهاجمی که با موفقیت از این آسیب‌پذیری بهره‌برداری کند، می‌تواند کنترل کامل سامانه از دور تحت‌تاثیر را در دست گیرد. پس از آن مهاجم می‌تواند برنامه‌ها را نصب کند. داده‌ها را مشاهده، تغییر، یا حذف کند یا حساب‌های جدیدی با حقوق کامل کاربر ایجاد کند. به‌روش‌های[4] دیوار آتش و پیکربندی‌های پیش‌فرض استاندارد برای دیوار آتش می‌تواند به حفاظت از شبکه در برابر حملاتی که خارج از محیط بنگاه سرچشمه می‌گیرند، کمک کند. به‌روش‌ها توصیه می‌کنند که سامانه‌هایی که متصل به اینترنت هستند دارای حداقل تعداد پورت‌های در معرض رخنه‌پذیری باشند.

این روزآمد امنیتی برای تمام نسخه‌های پشتیبانی ویندوز کارساز ۲۰۰۰ حیاتی بر شمرده شده است و برای نسخه‌های پشتیبانی ویندوز XP حرفه‌ای و ویندوز کارساز ۲۰۰۳ مهم تلقی شده است. برای اطلاعات بیشتر، به زیربند نرم‌افزار تحت‌تاثیر و غیر تحت‌تاثیر، در این بند مراجعه شود.

روزآمد امنیتی، آسیب‌پذیری را هنگام پردازش درخواست پروتکل دسترسی دایرکتوری سبک وزن (LDAP)[5] یا LDAPS[6] دستکاری‌شده خاص با تصحیح نحوه تخصیص و بازپس‌گیری حافظه توسط خدمات LDAP نشان می‌دهد.

---

1 - Active Directory
2 - Remote
3 - Active Directory Application Mode
4 - Best Practices
5 - Lightweight Directory Access Protocol
6 - LDAP over SSL

توصیه‌نامه. بیشتر مشتریان روزآمد خودکار را فعال کرده‌اند و به دلیل این که این روزآمد امنیتی بـه صـورت خودکار بارگیری و نصب خواهد شد نیاز به هیچ اقدامی ندارند. مشتریانی که روزآمد خودکار را فعال نکرده‌اند نیاز به وارسی روزآمد و نصب این روزآمد به صورت دستی دارند. برای اطلاعات در مورد گزینه‌های پیکربندی خاص در روزآمد خودکار، به مقاله ۲۹۴۸۷۱ پایگاه دانش مایکروسافت مراجعه شود.

برای مدیران سامانه و تاسیسات بنگاه یا کاربران نهایی که می‌خواهند این روزآمد امنیتی را به صورت دسـتی نصب کنند، مایکروسافت توصیه می‌کند که مشتریان روزآمـد را بلافاصـله بـا اسـتفاده از نـرم‌افـزار مـدیریت روزآمد، یا با وارسی برای روزآمد با استفاده از خدمات روزآمد مایکروسافت اعمال کنند.

همچنین به بخش، تشخیص و گسترش ابزارها و راهنماها، که بعد از این خبرنامه است، مراجعه شود.

بـــرای مشـــاهده توصـــیه کامـــل بـــه http://www.microsoft.com/technet/security/bulletin/ms09-018.mspx مراجعه شود.

آسیب‌پذیری‌ها و رخنه‌پذیری‌های متداول زیر به مثال توصیه مایکروسافت مرتبط است.

آسیب‌پذیری آزاد نامعتبر اکتیو دایرکتوری - CVE-2009-1138

آسیب‌پذیری اجرای کد از دور در پیاده‌سازی اکتیو دایرکتوری در ویندوز کارساز ۲۰۰۰ مایکروسـافت وجـود دارد. این آسیب‌پذیری به علت آزاد کردن نادرست حافظه در هنگام پردازش درخواست LDAP یـا LDAPS دستکاری‌شده خاص است. مهاجمی که با موفقیت از این آسیب‌پذیری بهره‌برداری می‌کند مـی‌توانـد کنتـرل کامل سامانه تحت‌تاثیر را در دست گیرد.

آسیب‌پذیری نشت حافظه اکتیو دایرکتوری - CVE-2009-1139

آسیب‌پذیری انکار خدمت در پیاده‌سازی اکتیو دایرکتوری در ویندوز کارساز ۲۰۰۰ و ویندوز کارسـاز ۲۰۰۳ وجود دارد. این آسیب‌پذیری در پیاده‌سازی حالت برنامه کاربردی اکتیو دایرکتوری (ADAM) زمانی کـه بـر روی ویندوز XP حرفه‌ای و ویندوز کارساز ۲۰۰۳ نصب شده است نیـز وجـود دارد. آسـیب‌پـذیری بـه علـت مدیریت نامناسب حافظه در طول اجرای انواع خاصی از درخواست‌های LDAP یا LDAPS اسـت. مهـاجمی که با موفقیت از این آسیب‌پذیری بهره‌برداری کند می‌تواند سبب جلوگیری از پاسخ کارساز تحت‌تاثیر شود.

ب-۲-۲مثال توصیه از سیسکو[1]

شناسانه سند: ۱۱۱۵۱۲

شناسانه توصیه: Cisco-sa-20100217-csa

http://www.cisco.com/warp/public/707/cisco-sa-20100217-csa.shtml

ویرایش: ۱.۲

آخرین روزآمد ۱۹ فوریه سال ۲۰۱۰ 1000 UTC (GMT)

1 - Cisco

برای انتشار عمومی ۱۷ فوریه سال ۲۰۱۰ 1600 UTC (GMT)

محتوا:

خلاصه:

محصولات تحت‌تاثیر:

جزئیات:

جزئیات بیشتر امتیازدهی آسیب‌پذیری:

اثر:

نسخه‌های نرم‌افزار و اصلاحیه‌ها:

راه‌کارها:

نرم‌افزار اصلاح‌شده به دست‌آمده:

بهره‌برداری و اطلاعیه‌های عمومی:

وضعیت این اطلاعیه: نهایی

توزیع:

تاریخ ویرایش:

روال‌های امنیتی سیسکو:

خلاصه:

مرکز مدیریت برای عامل امنیتی سیسکو[1] توسط آسیب‌پذیری پیمایش دایرکتوری[2] و آسیب‌پذیری تزریق SQL تحت‌تاثیر قرار گرفته است. بهره‌برداری موفقیت‌آمیز از آسیب‌پذیری پیمایش دایرکتوری می‌تواند به مهاجم اصالت‌سنجی‌شده اجازه مشاهده و بارگیری پرونده‌های دلخواه از کارساز میزبان مرکز مدیریت را دهد. بهره‌برداری موفقیت‌آمیز از آسیب‌پذیری تزریق SQL می‌تواند به مهاجم اصالت‌سنجی‌شده اجازه دهد تا دستورات SQL که می‌تواند سبب بی‌ثباتی محصول یا تغییرات در پیکربندی شود را اجرا کند.

علاوه بر این، عامل امنیتی سیسکو توسط آسیب‌پذیری انکار خدمت تحت‌تاثیر قرار می‌گیرد. بهره‌برداری موفقیت‌آمیز آسیب‌پذیری انکار خدمت عامل امنیتی سیسکو می‌تواند سبب ازکارافتادگی در سامانه تحت‌تاثیر شود. بهره‌برداری مکرر می‌تواند نتیجه شرایط انکار خدمت پایدار باشد.

این آسیب‌پذیری‌ها مستقل از یکدیگر هستند.

1 - The Management Center for Cisco Security Agents
2 - Directory traversal vulnerability

سیسکو روزآمدهای نرم‌افزاری رایگانی که به مقابله با این آسیب‌پذیری می‌پردازد را منتشر کرده است.

این توصیه در http://www.cisco.com/warp/public/707/cisco-sa-20100217-csa.shtml ارسال شده است.

ویرایش ۱.۰

۱۷ فوریه ۲۰۱۰

انتشار عمومی اولیه.

اطلاعات کامل در مورد گزارش‌دهی آسیب‌پذیری‌های امنیتی در محصولات سیسکو، دستیابی به کمک با رخدادهای امنیتی و ثبت نام برای دریافت اطلاعات امنیتی از سیسکو، در وبگاه سیسکو به نشانی http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html قابل دسترسی است. این وبگاه شامل دستورالعمل‌هایی برای درخواست‌های مطبوعات در مورد اعلامیه‌های امنیتی سیسکو است. تمامی توصیه‌های امنیتی سیسکو در http://www.cisco.com/go/psirt در دسترس است.

به‌روز شده در: ۱۹ فوریه ۲۰۱۰ شناسانه مستند: ۱۱۱۵۱۲

آسیب‌پذیری‌ها و رخنه‌پذیری‌های متداول زیر به مثال توصیه سیسکو مربوط است.

مرکز مدیریت برای آسیب‌پذیری پیمایش دایرکتوری عامل‌های امنیتی سیسکو

مرکز مدیریت برای عامل‌های امنیتی سیسکو توسط آسیب‌پذیری پیمایش دایرکتوری تحت‌تاثیر قرار گرفته است که به مهاجم اصالت‌سنجی‌شده اجازه مشاهده و بارگیری پرونده‌های دلخواه از کارساز میزبان مرکز مدیریت برای عامل‌های امنیتی سیسکو را می‌دهد.

این آسیب‌پذیری در شناسانه اشکال سیسکو CSCtd73275 مستند شده و به شناسانه CVE-2010-0146 آسیب‌پذیری و رخنه‌پذیری متداول (CVE) اختصاص داده شده است.

مرکز مدیریت برای آسیب‌پذیری تزریق SQL عامل‌های امنیتی سیسکو

مرکز مدیریت برای عامل‌های امنیتی سیسکو همچنین توسط آسیب‌پذیری تزریق SQL تحت‌تاثیر قرار گرفته است که می‌تواند به مهاجم اصالت‌سنجی‌شده اجازه دهد دستورات SQL که می‌تواند سبب بی‌ثباتی یا تغییر پیکربندی مرکز مدیریت برای عامل‌های امنیتی سیسکو شود را اجرا کند. این تغییرات پیکربندی می‌تواند منجر به تغییرات در خط‌مشی‌های امنیتی نقاط انتهایی شود. علاوه بر این، مهاجم می‌تواند حساب‌های کاربری مدیریت که در مرکز مدیریت برای عامل‌های امنیتی سیسکو یافت می‌شود را ایجاد کند، حذف کند، یا تغییر دهد.

این آسیب‌پذیری در شناسانه اشکال سیسکو CSCtd73290 مستند شده و به شناسانه CVE-2010-0147 آسیب‌پذیری و رخنه‌پذیری متداول (CVE) اختصاص داده شده است.

آسیب‌پذیری انکار خدمت عامل امنیتی سیسکو

عامل امنیتی سیسکو که توسط آسیب‌پذیری انکار خدمت تحت‌تاثیر قرار گرفته است می‌تواند به مهاجم غیرمجاز اجازه دهد تا سبب ازکارافتادگی سامانه با ارسال مجموعه‌های بسته‌های TCP شود.

یادآوری- تنها عامل امنیتی سیسکو نسخه ۵.۲ با آسیب‌پذیری انکار خدمت تحت‌تاثیر قرار گرفته است. ویندوزها و نسخه‌های سان سولاریس[1] عامل امنیتی سیسکو با آسیب‌پذیری انکار خدمت تحت‌تاثیر قرار نگرفته است.

این آسیب‌پذیری در شناسانه اشکال سیسکو شناسانه اشکال سیسکو CSCtd73290 مستند شده و به شناسانه CVE-2010-0148 آسیب‌پذیری و رخنه‌پذیری متداول (CVE) اختصاص داده شده است.

ب-۲-۳ مثال توصیه US-CERT

سامانه هشدار ملی فضای مجازی

هشدار امنیتی فنی فضای مجازی TA10-159A

آسیب‌پذیری نرم‌افزارهای فلش، ری‌در و آکروبات ادوبی

تاریخ انتشار اصلی: ۸ ژوئن ۲۰۱۰

آخرین ویرایش: ۲۹ ژوئن ۲۰۱۰

منبع: US-CERT

سامانه‌های تحت‌تاثیر

- نرم‌افزار ادوبی فلش پلیر ۱۰.۰.۴۵.۲ و نسخه‌های قبل از x.۱۰.
- نرم‌افزار ادوبی فلش پلیر ۹.۰.۲۶۲ و نسخه‌های قبل از x.۹.
- نرم‌افزار ادوبی ری‌در ۹.۳.۲ و نسخه‌های قبل از x.۹. ادوبی آکروبات ۹.۳.۲ و نسخه‌های قبل از x.۹

سایر محصولات ادوبی که از فلش پشتیبانی می‌کنند نیز می‌تواند آسیب‌پذیر باشد.

مرورکلی

به گفته ادوبی[2]، یک آسیب‌پذیری در نرم‌افزار ادوبی فلش وجود دارد. این آسیب‌پذیری فلش پلیر[3]، ری‌در[1]، آکروبات[2] و احتمالا سایر محصولاتی که از فلش پشتیبانی می‌کنند را تحت‌تاثیر قرار می‌دهد. مهاجم از دور می‌تواند این آسیب‌پذیری برای اجرای کدهای دلخواه بهره‌برداری کند.

1 - Sun Solaris
2 -Adobe
3 - Flash player

أ. شرح

توصیه امنیت ادوبی APSA10-01 آسیب‌پذیری در نرم‌افزار ادوبی فلش کـه فلـش پلیـر، ری‌در، آکروبـات را تحت‌تاثیر قرار می‌دهد، شرح می‌دهد. همچنین می‌تواند سایر محصولات که به طور مستقل از فلش پشتیبانی می‌کنند، مانند فتوشاپ، فتوشاپ لایت‌روم[3]، فریهاند MX [4]و فایر ورکز[5] را تحت‌تاثیر قرار دهد.

مهاجم می‌تواند از این آسیب‌پذیری با متقاعد کردن کاربر برای باز کردن محتوای فلش‌هـای دسـتکاری‌شـده خاص بهره‌برداری کند. محتوای فلش معمولا در یک صفحه وب میزبانی شده است، اما مـی‌توانـد در PDF و مستندات دیگر نیز تعبیه شود یا به صورت یک پرونده مستقل ارائه شود.

همان طور که در APSA10-01 اشاره شد، «گزارش‌هایی وجود دارد که این آسیب‌پذیری بـه طـور فعـال در نرم‌افزار های ادوبی فلش پلیر، و ادوبی ری‌در و آکروبات مورد بهره‌برداری قرار گرفته است.»

اطلاعات افزوده در یادداشت آسیب‌پذیری VU # 486225، US-CERT موجود است.

ب. اثر

اگر کاربری محتوای فلش دستکاری‌شده خاص را باز کند، مهاجم از دور می‌تواند کدهای دلخواه را اجرا کند.

ج. راه‌حل

روزآمد فلش

خبرنامه امنیتی ادوبی APSB10-14 روزآمد فلش پلیر ۱۰.۱.۵۳.۶۴ یا ۹.۰.۲۷۷.۰ را توصیه می‌کند. این کار سبب روزآمد افزوده مرورگر وب و اکتیو ایکس کنترل[6] خواهد شد، اما پشتیبانی فلش در نرم‌افزارهای ادوبـی ری‌در، آکروبات یا سایر محصولات را روزآمد نمی‌کند.

روزآمد ری‌در و آکروبات

خبرنامه امنیتی ادوبی APSB10-15 روزآمد ۹.۳.۳ یا ۸.۲.۳ نسخه ری‌در و آکروبات را توصیه می‌کنـد، ایـن کار پشتیبانی فلش در ادوبی ری‌در و آکروبات را روزآمد خواهد کرد.

به منظور کاهش رخنه‌پذیری در برابر این آسیب‌پذیری و سایر آسیب‌پذیری‌های فلش، فنون کاهش زیر را در نظر بگیرید.

---

1 - Reader
2 - Acrobat
3 - Photoshop Lightroom
4 - Freehand MX
5 - Fireworks.
6 - Active X control

غیر فعال کردن فلش در مرورگر وب

فلش را حذف کنید یا وبگاه‌های مجاز به اجرای فلش را محدود کنید. تا حد امکان، تنها محتوای فلش قابل اعتماد در دامنه‌های مورد اعتماد را اجرا کنید. برای اطلاعات بیشتر، به امن‌سازی مرورگر وب مراجعه شود.

غیر فعال کردن فلش در نرم‌افزارهای ادوبی ری‌در و آکروبات

غیر فعال کردن فلش در نرم‌افزار ادوبی ری‌در حملاتی که با تکیه بر محتوای فلش در پرونده PDF تعبیه‌شده است را کاهش می‌دهد. غیرفعال‌کردن پشتیبانی سه بعدی (3D)[1] و چندرسانه‌ای به طور مستقیم به این آسیب‌پذیری نمی‌پردازد، بلکه سبب کاهش بیشتر آسیب‌پذیری می‌شود و در نتیجه به جای ازکارافتادگی، یک پیام خطای کاربر پسندتر را ارائه می‌دهد. برای غیر فعال کردن پشتیبانی از فلش و 3D و چندرسانه‌ای در نرم‌افزار ادوبی ری‌در ۹ دسترسی به این پرونده‌ها را حذف کنید، تغییر نام دهید یا از بین ببرید.

ویندوز مایکروسافت

“%ProgramFiles%\Adobe\Reader 9.0\Reader\authplay.dll”

“%ProgramFiles%\Adobe\Reader 9.0\Reader\rt3d.dll”

سامانه عامل مک اپل **X**[2]

“/Applications/AdobeReader9/AdobeReader.app/Contents/Frameworks/AuthPlayLib.bundle”

“/Applications/AdobeReader9/AdobeReader.app/Contents/Frameworks/Adobe3D.framework”

GNU / لینوکس[3] (مکان‌ها می‌تواند در توزیع‌های مختلف متفاوت باشد)

/"opt/Adobe/Reader9/Reader/intellinux/lib/libauthplay.so"

/"opt/Adobe/Reader9/Reader/intellinux/lib/librt3d.so"

مکان‌های پرونده برای نرم‌افزار ادوبی آکروبات یا سایر محصولات ادوبی که شامل پشتیبانی فلش و 3D و چندرسانه‌ای هستند می‌تواند مختلف باشد. غیر فعال کردن این افزوده‌ها کارکرد را کاهش خواهد داد و در برابر محتوای فلش قرارگرفته در وبگاه‌ها، محافظتی نمی‌کند. بسته به برنامه روزآمد برای محصولات به غیر از فلش پلیر، پشتیبانی فلش و 3D و چندرسانه‌ای را غیر فعال کنید، مگر این که این موارد کاملا مورد نیاز باشد.

پیشگیری مرورگر اینترنت اکسپلورر[4] برای بازکردن مستندات PDF به طور خودکار

1 - Three dimensional
2 - Apple Mac OS X
3 - Linux
4 - Internet explorer

نصب‌کننده نرم‌افزارهای ادوبی ری‌در و آکروبات اینترنت اکسپلورر را برای باز کردن پرونده‌های PDF به طور خودکار بدون هیچ‌گونه تعامل با کاربر، پیکربندی می‌کند. این رفتار می‌تواند به گزینه ایمن‌تری بازگردد که کاربر را با وارد کردن مورد زیر به عنوان یک پرونده .REG حفظ می‌کند.

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\AcroExch.Document.7]
"EditFlags" = hex:00,00,00,00
```

غیرفعال‌کردن نمایش مستندات PDF در مرورگر وب

پیشگیری از باز کردن مستندات PDF در مرورگر وب تاحدودی سبب کاهش این آسیب‌پذیری خواهد شد. اگر این راه‌کار به کار رود، می‌تواند آسیب‌پذیری‌های آینده را نیز کاهش دهد.

برای پیشگیری از بازکردن مستندات PDF به طور خودکار در مرورگر وب، موارد زیر را انجام دهید:

الف) نرم‌افزار ادوبی آکروبات ری‌در را باز کنید؛

ب) گزینگان (منوی)[1] ویرایش را باز کنید؛

ج) گزینه تنظیمات را انتخاب کنید.

د) بخش اینترنت را انتخاب کنید.

ه) تیک «نمایش PDF در مرورگر» را بردارید.

غیر فعال کردن جاوا اسکریپت در نرم‌افزارهای ادوبی ری‌در و آکروبات

غیر فعال کردن جاوا اسکریپت، برخی حفاظت‌های بیشتر را در برابر حملات ارائه می‌کند. جاوا اسکریپت آکروبات می‌تواند با استفاده از گزینگان تنظیمات غیر فعال شود:

(Edit - > Preferences - > JavaScript; uncheck Enable AcrobatJavaScript)

فعالسازی پیشگیری از اجرای داده (DEP)[2] در ویندوز مایکروسافت

فعالسازی DEP در نسخه‌های پشتیبانی‌شده ویندوز را مد نظر قرار دهید. DEP نباید به عنوان یک راه‌کار کامل برطرف‌سازی در نظر گرفته شود، اما می‌تواند اجرای کد عرضه‌شده توسط مهاجم را در برخی موارد کاهش دهد. مایکروسافت اطلاعات فنی با جزئیات در مورد DEP را در تحقیقات امنیتی و پست‌های وبلاگ دیفنس[3] «درک DEP به عنوان یک فناوری کاهش» قسمت ۱ و قسمت ۲ منتشر کرده است. استفاده از DEP باید همراه با به کارگیری وصله‌ها یا سایر راه‌های کاهش شرح‌داده‌شده در این مستند در نظر گرفته شود.

1 - Menu
2 - Data Execution Prevention
3 - Defence

به مستندات PDF منابع غیر قابل اعتماد دسترسی پیدا نکنید

مستندات PDF ناآشنا یا غیرمنتظره، به خصوص مستنداتی که در وبگاه‌ها قرار گرفته‌اند یا به عنوان پیوست‌های رایانامه تحویل شده است را باز نکنید. به نکته امنیت فضای مجازی ST04-010 مراجعه شود.

د. منابع

- توصیه امنیتی برای نرم‌افزارهای فلش پلیر، ادوبی ری‌در و آکروبات-

http://www.adobe.com/support/security/advisories/apsa10-01.html

- روزآمد امنیتی برای نرم‌افزار ادوبی فلش پلیر –

security/bulletins/apsb10-14.html/http://www.adobe.com/support

- روزآمد امنیتی برای نرم‌افزارهای ادوبی ری‌در و ادوبی آکروبات-

http://www.adobe.com/support/security/bulletins/apsb10-15.html

- آزمایشگاه‌های ادوبی - نرم‌افزار فلش پلیر ۱۰ قبل از انتشار-

http://labs.adobe.com/technologies/flashplayer10/

- نکته آسیب‌پذیری US-CERT VU # 486225–

http://www.kb.cert.org/vuls/id/486225

- امن‌سازی مرورگر وب شما –

http://www.us-cert.gov/reading_room/securing_browser/

- آشنایی با DEP به عنوان بخشی از فناوری کاهش قسمت ۱ –

http://blogs.technet.com/b/srd/archive/2009/06/05/understanding-dep-as-a-mitigation-technology-part-1.aspx

- آشنایی با DEP به عنوان بخشی از فناوری کاهش قسمت ۲ -

http://blogs.technet.com/b/srd/archive/2009/06/12/understanding-dep-as-a-mitigation-technology-part-2.aspx

- CVE-2010-1297 –

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1297<

بازخوردها می‌تواند به US-CERT ارائه شود.

تاریخچه ویرایش

انتشار اولیه: ۸ ژوئن ۲۰۱۰

شناسانه CVE اضافه‌شده، روزآمدشده برای APSB10-14: ۱۱ ژوئن ۲۰۱۰

روزآمدشده برای APSB10-15 : ۲۹ ژوئن ۲۰۱۰

آخرین روزآمد ۲۹ ژوئن ۲۰۱۰

ب-۳ هماهنگ‌کننده‌های به رسمیت شناخته‌شده در سطح جهانی

در زیر فهرستی غیر جامعی از هماهنگ‌کننده‌های به رسمیت شناخته‌شده در سطح جهانی در زمان آخرین روزآمد این استاندارد ارائه شده است.

CERT Australia — www.cert.gov.au

CERT/CC (Software Engineering Institute (SEI) CERT Program of Carnegie Mellon University) — www.cert.org

CERT-FI (Finnish national Computer Emergency Response Team) — http://www.cert.fi/en/

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) — www.jpcert.or.jp/english/

ب-۴ منابع افزوده

شمارش نقاط ضعف عمومی (CWE)[1] - روشی واحد برای تعیین نقاط ضعف نرم‌افزار ارائه می‌کند-

http://cwe.mitre.org

پروژه امنیتی برنامه کاربردی وب باز (OWASP) – روش‌هایی برای درک و آزمون برای نقاط ضعف برنامه‌های کاربردی وب ارائه می‌کند-

https://www.owasp.org/index.php/Main_Page

1 - Common Weakness Enumeration

کتابنامه

[1] ISO/IEC 15408-1:2009, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

[2] ISO/IEC 15443-1:2012, Information technology — Security techniques — Security assurance framework – Part 1: Introduction and concepts

[3] ISO/IEC 19770-1:2012, Information technology — Software asset management — Part 1: Processes and tiered assessment of conformance

[4] ISO/IEC 19791:2010, Information technology — Security techniques — Security assessment of operational systems

[5] ISO/IEC 20000-1:2011, Information technology — Service management — Part 1: Service management system requirements

[۶] استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی - الزامات

[۷] استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی –آیین‌کار مدیریت امنیت اطلاعات

[۸] استاندارد ملی ایران شماره ۲۷۰۳۵: سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی – مدیریت رخداد امنیت اطلاعات

[9] ITU-T X.1521 (04/2011), Common Vulnerability Scoring System (ITU-T Recommendations

[۱۰] استاندارد ملی ایران شماره ۲۷۰۱۰: سال ۱۳۹۲، فناوری اطلاعات -فنون امنیتی -مدیریت امنیت اطلاعات برای ارتباطات درون بخشی و درون سازمانی