فهرست آسیب‌پذیری‌های شناسایی‌شده در محصولات پرکاربرد شرکت‌های مطرح، هفته‌ی اول دی ۹۹

شماره	شناسه	شرکت	امتیاز	سطح خطر	نوع	محصول آسیب‌پذیر	نوع محصول	بردار دسترسی	نیاز به احراز هویت	توضیحات	وضعیت رفع
۱	CVE-2020-35608	مایکروسافت	۵/۵	متوسط	خرابی حافظه	Azure Sphere	Cloud Software	شبکه‌ی مجاور	دارد_ تک مرحله‌ای	نسخه‌ی آسیب‌پذیر: ۲۰/۰۷	تعیین‌نشده
۲	CVE-2020-35609	مایکروسافت	۵/۵	متوسط	خرابی حافظه	Azure Sphere	Cloud Software	شبکه‌ی مجاور	دارد_ تک مرحله‌ای	نسخه‌ی آسیب‌پذیر: ۲۰/۰۵	تعیین‌نشده
۳	CVE-2020-3999	Vmware	۳/۵	پایین	منع سرویس	ESXi Workstation Fusion Cloud Foundation	Virtualization Software	شبکه‌ی مجاور	دارد_ تک مرحله‌ای	_	وصله‌ی رسمی

پیوست

معیارهای مختلف برای توصیف یک آسیب‌پذیری

شناسه‌ی آسیب‌پذیری

شناسه‌ی آسیب‌پذیری (یا همان CVE)، کد منحصر به فردی است که به هر آسیب‌پذیری امنیتی شناسایی‌شده و با هدف ردیابی آن، اختصاص داده می‌شود.

امتیاز آسیب‌پذیری

سیستم امتیازدهی آسیب‌پذیری عام (CVSS)، یک چارچوب باز برای انتقال مشخصات و شدت آسیب‌پذیری‌های نرم‌افزاری است. این سیستم امتیازدهی از سه گروه: پایه، زمانی (موقتی) و محیطی تشکیل شده است. گروه پایه، ویژگی‌های ذاتی یک آسیب‌پذیری را نشان می‌دهد که با گذشت زمان و در محیط‌های مختلف ثابت است. گروه زمانی، منعکس‌کننده‌ی آن دسته از ویژگی‌های یک آسیب‌پذیری است که با گذشت زمان تغییر می‌کنند و در نهایت، گروه محیطی، ویژگی‌های منحصر به محیط کاربری را بیان می‌کند. امتیازهای اختصاص‌یافته به آسیب‌پذیری‌ها در این سیستم، بازه‌ی صفر تا ۱۰ را شامل می‌شود. در این سند، امتیاز پایه‌ی آسیب‌پذیری‌ها ارائه می‌شود.

سطح خطر آسیب‌پذیری

برای برخی اهداف، داشتن نمایشی متنی از امتیازهای عددی پایه، زمانی و محیطی مفید خواهد بود. سطح خطر آسیب‌پذیری‌ها با توجه به امتیازهای CVSS به صورت زیر تعریف می‌شود:

امتیاز CVSS	سطح خطر
۰/۰	بدون خطر
۰/۱ ـ ۳/۹	خطر پایین
۴/۰ ـ ۶/۹	خطر متوسط
۷/۰ ـ ۸/۹	خطر بالا
۹/۰ ـ ۱۰/۰	بحرانی

بردار دسترسی

این معیار، منعکس‌کننده‌ی زمینه‌ای است که به موجب آن بهره‌برداری از آسیب‌پذیری ممکن می‌شود. در حالت کلی، بهره‌برداری از آسیب‌پذیری‌ها به چهار صورت امکان‌پذیر است:

- شبکه‌ــ از راه دور: در این حالت، امکان بهره‌برداری از آسیب‌پذیری از طریق شبکه‌های اینترنتی و به صورت راه دور وجود دارد.
- شبکه‌ی مجاور: در این حالت نیز، بهره‌برداری از آسیب‌پذیری به پشته‌ی شبکه متکی است، با این حال، انجام حمله به توپولوژی مجاور مانند بلوتوث، IEEE 802.11، یا زیرشبکه‌ی IP محلی، محدود می‌شود.
- محلی: در این حالت، بهره‌برداری از آسیب‌پذیری به پشته‌ی شبکه محدود نبوده و مسیر مهاجم، از طریق قابلیت‌های خواندن / نوشتن / اجرا است. در این روش، مهاجم از طریق دسترسی محلی به هدف (مانند صفحه‌ی کلید، کنسول)، و یا از راه دور (مانند پروتکل SSH)، و یا تعامل با کاربر (فریب کاربران برای بازکردن فایل‌های مخرب)، اقدام به بهره‌برداری از آسیب‌پذیری‌ها می‌کند.
- فیزیکی: در این حالت، مهاجم برای بهره‌برداری از آسیب‌پذیری‌ها، نیاز به لمس و دستکاری فیزیکی محصول آسیب‌پذیر دارد.

نیاز به احراز هویت

این معیار میزان امتیازاتی را که یک مهاجم، برای بهره‌برداری موفقیت‌آمیز از یک آسیب‌پذیری به آنها نیاز دارد، توصیف می‌کند. در حالت کلی، این معیار به سه گروه زیر تقسیم می‌شود:

- ندارد: مهاجم برای انجام حمله، نیازی به دسترسی به تنظیمات یا فایل‌های سیستم آسیب‌پذیر ندارد.
- دارد‌ــ تک مرحله‌ای: برای بهره‌برداری از آسیب‌پذیری، مهاجم به امتیازاتی نیاز دارد که قابلیت‌های اساسی کاربر، مانند تنظیمات و فایل‌های سیستم، را تحت تأثیر قرار می‌دهند. یک مهاجم با امتیازات پایین، تنها توانایی دسترسی به منابع غیرحساس را دارد.
- دارد‌ــ چند مرحله‌ای: در این حالت، مهاجم برای بهره‌برداری از آسیب‌پذیری، به امتیازاتی نیاز دارد که کنترل قابل توجهی را بر مؤلفه‌ی آسیب‌پذیر دارند. در این حالت، امکان دسترسی به تنظیمات و فایل‌های کل مؤلفه برای مهاجم فراهم می‌شود.