بسمه تعالی

مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

گزارش آسیب پذیری پروتکل SMBv3

گزارش آسیب پذیری

فهرست مطالب

۱ مقدمه

پروتکل Server Message Block که به اختصار SMB نامیده می‌شود، یک پروتکل شبکه‌ای متخص سیستم‌های مبتنی بر ویندوز است که قابلیت اشتراگ گذاری بین سیستم‌های موجود در یک شبکه را فراهم می‌کند. در حال حاضر نسخه ۳ این پروتکل استفاده می‌شود که از زمان انتشار ویندوز ۸ و سرور ۲۰۱۲ ارائه شده است. به توصیه مایکروسافت نسخه‌های ۲ و ۳ برای اشکال زدایی ارائه شده‌اند و به همین خاطر توصیه می‌شود که این پروتکل‌ها بر روی سیستم غیر فعال باشند.

۲ آسیب پذیری CVE-2020-0796

در تاریخ ۱۲ مارس سال ۲۰۲۰ شرکت مایکروسافت اعلام کرد که یک آسیب‌پذیری جدی سیستم‌های ویندوزی در حال استفاده از پروتکل SMBV3 را تهدید می‌کند. بنابر توضیحات شرکت مایکروسافت این آسیب‌پذیری بر روی نحوه رفتار SMBV3 با درخواست‌های بخصوص رخ می‌دهد. یک مهاجم غیر احراز هویت‌شده می‌تواند با ارسال درخواست‌های دستکاری‌شده خاص به سرور SMBV3 آن را مورد حمله قرار داده و از آسیب‌پذیری بهره ببرد. بهره‌جویی موفق از این آسیب‌پذیری مهاجم را قادر به اجرای کد بر روی هم سرور و هم کاربر SMB می‌سازد. با این حال مطابق با گزارش‌های منتشر شده ، کد بهره برداری این آسیب پذیری تحت عنوان نرم افزارهای متن باز در اینترنت موجود است و سیستم‌هایی که این آسیب پذیری را دارند، به راحتی مورد حمله واقع می‌شوند.

آسیب پذیری به گونه‌ای است که فرد مهاجم می‌تواند کنترل یک ماشین راه دور را به دست بگیرد. کلیه نسخه‌های ویندوز با شماره ساخت ۱۹۰۳ و ۱۹۰۹ بالقوه امکان نفوذ پذیری به خاطر این آسیب پذیری را دارند.

۳ راه حل

خوشبختانه وصله‌ی این آسیب پذیری به شماره KB4551762 از طرف مایکروسافت ارائه شده است. به همین خاطر لازم است در قدیمی بودن سیستم‌های عامل، به روزرسانی خودکار در اسرع وقت انجام شود. همچنین توصیه شده است، برخی از ویژگی‌های این پروتکل غیر فعال شوند که در ادامه درباره آن‌ها توضیح داده می‌شود.

۳-۱ غیر فعال کردن پروتکل

برای این کار در PowerShell دستور زیر را اجرا کنید تا ابتدا وضعیت پروتکل معلوم شود و سپس غیر فعال شود.

```
Get-SmbServerConfiguration | Select EnableSMB2Protocol
Set-SmbServerConfiguration -EnableSMB2Protocol $false
```

۳-۲ غیر فعال کردن فشرده سازی پروتکل

برای این کار دستور زیر را اجرا کنید.

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
DisableCompression -Type DWORD -Value 1 -Force
```

۴ منابع

[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796

[2] https://www.us-cert.gov/ncas/current-activity/2020/06/05/unpatched-microsoft-systems-vulnerable-cve-2020-0796

[3] https://support.microsoft.com/en-us/help/4551762/windows-10-update-kb4551762