**رفع مشکل امنیتی پروتکل smb**

مایکروسافت یک بسته امنیتی بسیار مهم را برای پروتکل SMBv3 منتشر کرده است؛ اخیرا یک مشکل امنیتی بسیار خطرناک در این پروتکل مشاهده شده است که به مهاجمان اجازه میدهد تا بدافزارهایی که قابلیت تکثیر (worm) ایجاد کنند، که بعد از آلوده کردن یک سیستم، بقیه سیستم های متصل به آن شبکه را نیز آلوده می کنند.

**درباره آسیب پذیری SMBv3**

این آسیب پذیری با شماره CVE-2020-0796 ثب شده است و می توانید با این شماره آن را جستجو کنید. این آسیب پذیری نقص اجرای کد از راه دور است که ویندوز 10 نسخه 1909 و 1903 و ویندوز سرور نسخه 1903 و 1909 را تحت تاثیر قرار می دهد.

**پروتکل Server Message Block - SMB**

پروتکل SMB روی پورت 445 TCP کار می کند و پروتکلی است که برای اشتراک گذاری فایل ها، چاپگرها، پورت های سریال و سایر منابع در شبکه طراحی شده است. از این پروتکل در سیستم های ویندوزی استفاده می شود.

**بسته بروز رسانی امنیتی**

بسته امنیتی برای آخرین آسیب پذیری با کد [**KB4551762**](https://support.microsoft.com/en-us/topic/servicing-stack-update-for-windows-10-version-1903-and-1909-march-10-2020-5a648584-4e14-a8cc-0a45-2ea36dd8b8ca) در سایت مایکروسافت ارائه شده و اکنون قابل دسترس است. روش کار فعلی پروتکل SMBv3 به این صورت است که درخواست ها را با فشرده سازی هدرها Headers مدیریت می کند، که این امر باعث شده تا مهاجمی که احراز هویت نشده است کدهای خطرناکی را چه در سمت [سرور](https://parspack.com/servers)و چه در سمت کاربر با دسترسی SYSTEM اجرا کند.

**قبل از نصب به روز رسانی**

مایکروسافت شدیدا توصیه می کند که قبل از بروز رسانی آخرین سرویس به روز رسانی پشته Servicing Stack Update- SSU را برای سیستم عامل خود نصب کنید، سپس آخرین بروز رسانی باقیمانده Latest Cumulative Update - LCU را نصب کنید. SSU قابلیت اطمینان فرآیند به روزرسانی را برای کاهش مشکلات احتمالی در حین نصب LCU و استفاده از اصلاحات امنیتی مایکروسافت بهبود می بخشد. اگر برای بروز رسانی از Windows Update استفاده می کنید آخرین آپدیت SSU - KB4541338 به صورت خودکار پیشنهاد می شود. برای نصب جداگانه این بسته کاتالوگ بروز رسانی مایکروسافت را جستجو کنید.

**نصب بسته امنیتی مایکروسافت**

برای دانلود و نصب بسته امنیتی مایکروسافت از سه روش به صورت زیر می توانید اقدام کنید :

|  |  |  |
| --- | --- | --- |
| کانال دسترسی | فعال بودن | گام بعدی |
| Windows Update and Microsoft Update | بله | این بروزرسانی به صورت خودکار دانلود و نصب می شود |
| Microsoft Update Catalog | بله | برای نصب جداگانه و مستقل بسته امنیتی برای این بروزرسانی به سایت [کاتالوگ](https://catalog.update.microsoft.com/Search.aspx?q=KB4551762) [مایکروسافت](https://catalog.update.microsoft.com/Search.aspx?q=KB4551762) مراجعه کنید. |
| Windows Server Update Services (WSUS) | بله | اگر پیکربندی محصولات و دسته بندی ها را در WSUS به صورت زیر تنظیم کرده باشید، این بروزرسانی به صورت خودکار همگام سازی می شود : Product: Windows 10, version 1903 and later Classification: Security Updates |

**پیدایش مشکل امنیتی**

ویندوز 10 و ویندوز سرور چندی پیش مشکلی داشتند که برای رفع آن یک به روز رسانی برای فشرده سازی هدرها منتشر شد. فشرده سازی هدرها Headers به عنوان یک ویژگی جدید در تاریخ May 2019 به پروتکل های آسیب دیده ویندوز 10 و ویندوز سرور اضافه شد. این به روز رسانی برای فشرده سازی اندازه پیام های رد و بدل شده بین یک سرور و کاربرانی که به آن متصل هستند ، طراحی شده است.

**نحوه استفاده از آسیب پذیری**

به نقل از مایکروسافت : برای استفاده از این آسیب پذیری در یک سرور، یک مهاجم احراز هویت نشده بسته های دستکاری شده را به یک سرور SMB هدف ارسال می کند. برای استفاده از آسیب پذیری در سمت کاربر نیز مهاجم غیر مجاز و احراز هویت نشده، یک سرور SMB مخرب و آلوده را راه اندازی و تنظیم می کند و کاربر را برای اتصال به آن سرور متقاعد می کند. به روزرسانی امنیتی با تصحیح نحوه برخورد پروتکل SMBv3 به این درخواست های خاص دستکاری شده ، آسیب پذیری را برطرف می کند.

**ابزارهای استفاده از آسیب پذیری**

در زمان نوشتن این مطلب فقط یک exploit برای استفاده از این آسیب پذیری وجود دارد. هکر ها با استفاده از مهندسی معکوس بسته های امنیتی ارائه شده و پیدا کردن بردارهای حمله های احتمالی بدافزارهای پیشرفته ای را تولید کنند. تا امروز ، نزدیک به 48000 سیستم ویندوز در برابر آخرین آسیب پذیری فشرده سازی SMB، آسیب پذیر هستند و از طریق اینترنت قابل دسترسی هستند.

**پایان**

اکنون بسته به روز رسانی نقص امنیتی SMBv3 Wormable برای نسخه های آسیب دیده موجود است و شدیدا پیشنهاد می شود که در اسرع وقت این به روز رسانی را نصب کنید. اگر امکان نصب فوری این بسته امنیتی را ندارید، پیشنهاد می شود که حداقل سرویس SMB یا ویژگی فشرده سازی آن را غیر فعال کنید و پورت های SMB را برای هر دو ترافیک ورودی و خروجی ببندید تا از دسترسی استفاده از راه دور جلوگیری کنید.

**سوالات متداول :**

**مشکل امنیتی جدید پروتکل SMB چیست؟**

آخرین مشکل امنیتی پروتکل SMB برای نسخه v3 این پروتکل می باشد و بر روی ویژگی فشرده سازی بسته ها Packets کار می کند. این ویژگی به تازگی به ویندوز برای بهبود عملکرد پروتکل ها اضافه شده است.

**مهاجم یا هکر چطور مشکل امنیتی جدید پروتکل SMB استفاده می کند؟**

مهاجم به صورت غیر مجاز و احراز هویت نشده، بسته Packets های دستکاری شده را به سرور SMB ارسال می کند، یا اینکه یک سرور SMB آلوده را راه اندازی می کند تا کاربر به آن متصل شود.

**چطور مشکل امنیتی SMBv3 را رفع کنم؟**

کافیست فقط ویندوز خود را از Windows Update به روز رسانی کنید. اگر از WSUS در شبکه خود استفاده می کنید، حتما سرور WSUS را به آخرین به روز رسانی Sync کنید و آخرین آپدیت ها را در سیستم کاربران نصب کنید.

**مشکل امنیتی Wormable SMBv3 در چه سیستم عاملهایی کار می کند؟**

ویندوز ۱۰ نسخه ۱۹۰۹ و ۱۹۰۳ و ویندوز سرور نسخه ۱۹۰۹ و ۱۹۰۳

**چطور سرویس SMB را غیر فعال کنم؟**

در  وب سایت [مایکروسافت](https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3)  به صورت کامل فعال و غیر فعال کردن تمام نسخه های SMB در تمام نسخه های ویندوز توضیح داده شده است.