بسمه تعالی

تاریخ تحریر 21/12/98

گزارش آسیب پذیری در Microsoft Server Message Block v3 با شماره CVE-2020-0796

آسیب پذیری مذکور در تاریخ 10 مارس 2020 توسط شرکت مایکروسافت منتشر شده است که از نوع RCE میباشد. مهاجم می تواند با ارسال یک پکت خاص به سمت سرور با سرویس دهنده SMBv3 آسیب پذیر، از آن سوءاستفاده نماید. همچنین درمورد کاربران Client، مهاجم باید قربانی را متقاعد کند تا با یک سرور مخرب که توسط مهاجم پیکربندی شده است ارتباط برقرار کند. سوء استفاده مهاجم از آسیب پذیری مذکور به او این امکان را میدهد تا کد دلخواه خود را بر روی سیستم قربانی اجرا کند.

بر اساس شواهد به نظر می رسد این نقص ناشی از آسیب پذیری سرریز بافر میباشد که به دلیل خطا در handling پکت های فشرده رخ می دهد. محققان به دلیل شباهت های این آسیب پذیری به آسیب پذیری EternalBlue که چندی پیش به طور گسترده مورد سوء استفاده قرار گرفت و مهم ترین آن CVE-2017-0144 بوده که در حملات باج افزار WannaCry مورد استفاده قرار گرفت، این آسیب پذیری را به عنوان EternalDarkness نام گذاری کرده اند.

نسخه های آسیب پذیر

product	Version
Windows Server	**Version 1903 (Server Core Installation)**
Windows Server	**Version 1909 (Server Core Installation)**
Windows 10	**Version 1903 for 32-bit Systems**
Windows 10	**Version 1903 for ARM64-based Systems**
Windows 10	**Version 1903 for x64-based Systems**
Windows 10	**Version 1909 for 32-bit Systems**
Windows 10	**Version 1909 for ARM64-based Systems**
Windows 10	**Version 1909 for x64-based Systems**

راه حل

در حال حاضر هیچ وصله امنیتی برای مرتفع سازی این آسیب پذیری منتشر نشده است و مایکروسافت نیز فعلا یک دستورالعمل را به عنوان راهکار موقت برای پیشگیری از این آسیب پذیری ارائه داده است. این دستورالعمل شامل یک دستور در محیط PowerShell است که فشرده سازی را برای SMBv3 Server غیر فعال می کند تا مهاجم نتواند از آسیب پذیری سوءاستفاده کند:

```
Set-ItemProperty –Patch “KHLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters” DisableCompression –Type DWORD –Value 1 –Force
```

علاوه بر غیرفعال کردن فشرده سازی ، مایکروسافت توصیه می کند ترافیک ورودی و خروجی درگاه TCP 445 در فایروال ها مسدود شوند.

همچنین شما می توانید اطلاعات بیشتری درمورد راه حل های ارائه شده توسط مایکروسافت را از لینک زیر دریافت نمایید.

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV200005

منبع

https://www.tenable.com/blog/cve-2020-0796-wormable-remote-code-execution-vulnerability-in-microsoft-server-message-block