بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

آسیب‌پذیری اجرای کد از راه دور ویندوز سرور

هشدار

شناسه سند	MaherReport_13990726-01
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۳۹۹/۰۷/۲۵
طبقه‌بندی سند	**عادی**

تهران، میدان آرژانتین، ابتدای بلوار بیهقی، نبش خیابان شانزدهم، ساختمان شماره ۱، سازمان فناوری اطلاعات ایران

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ مقدمه

مایکروسافت در ۱۳ اکتبر، اطلاعیه‌ای در خصوص یک آسیب‌پذیری بحرانی در IPv6 stack منتشر کرد. این آسیب‌پذیری با شناسه CVE-2020-16898 دارای امتیاز 9.8 براساس CVSSv3 است. نفوذگران می‌توانند با اکسپلویت این آسیب‌پذیری کد دلخواه خود را از راه دور در سیستم‌های تحت‌تاثیر آسیب‌پذیری هدف اجرا نمایند یا موجب انکار سرویس در آن‌ها شوند. مایکروسافت در به‌روزرسانی اکتبر ۲۰۲۰ وصله این آسیب‌پذیری را منتشر کرده است.

۲ میزان خطر

این آسیب‌پذیری ویندوز ۱۰، ویندوز سرور ۲۰۱۹ و هسته‌های نسخه ۲۰۰۴، ۱۹۰۹ و ۱۹۰۳ را تحت تاثیر قرار می‌دهد. لیست کامل محصولات تحت‌تاثیر در جدول ۱ نمایش داده شده است. بر اساس تحقیقات Mcafee، کاربران ویندوز ۱۰ پرخطرترین گروه تحت تاثیر این آسیب‌پذیری هستند.

۳ رفع آسیب‌پذیری

بهترین روش برای رفع این آسیب‌پذیری‌ها به‌روزرسانی محصولات تحت تاثیر آسیب‌پذیری (جدول ۱) است. اگر امکان به‌روزرسانی وجود نداشته باشد. می‌توان با استفاده از دستور زیر در PowerShell ویندوز ICMPv6 RDNSS را غیر فعال کرد و مانع از حمله شد.

```
netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=disable
```

جدول ۱- لیست محصولات نیازمند به‌روزرسانی

نام محصول	لینک دانلود به‌روزرسانی
ویندوز ۱۰	نسخه ۱۷۰۹ سیستم‌های ۳۲ بیتی
ویندوز ۱۰	نسخه ۱۷۰۹ سیستم‌های ARM64
ویندوز ۱۰	نسخه ۱۷۰۹ سیستم های x64
ویندوز ۱۰	نسخه ۱۸۰۳ سیستم‌های ۳۲ بیتی

ویندوز ۱۰	نسخه ۱۸۰۳ سیستم‌های ARM64
ویندوز ۱۰	نسخه ۱۸۰ سیستم‌هایx64
ویندوز ۱۰	نسخه ۱۸۰۹ سیستم‌های ۳۲ بیتی
ویندوز ۱۰	نسخه ۱۷۰۹ سیستم‌های ARM64
ویندوز ۱۰	نسخه ۱۸۰۹ سیستم‌هایx64
ویندوز ۱۰	نسخه ۱۹۰۳ سیستم‌های ۳۲ بیتی
ویندوز ۱۰	نسخه ۱۹۰۳ سیستم‌های ARM64
ویندوز ۱۰	نسخه ۱۹۰۳ سیستم‌های x64
ویندوز ۱۰	نسخه ۱۹۰۹ سیستم‌های ۲۳ بیتی
ویندوز ۱۰	نسخه ۱۹۰۹سیستم‌های ARM64
ویندوز ۱۰	نسخه ۱۹۰۹نسیستم‌های x64
ویندوز ۱۰	نسخه ۲۰۰۴ سیستم‌های۳۲ بیتی
ویندوز ۱۰	نسخه ۱۹۰۹سیستم‌های ARM64
ویندوز ۱۰	نسخه ۱۹۰۹سیستم‌هایX64
ویندوز ۲۰۱۹	ویندوز سرور ۲۰۱۹
ویندوز ۲۰۱۹	ویندوز سرور ۲۰۱۹ (نصب از هسته)
ویندوز سرور	ویندوز سرور نسخه ۱۹۰۳(نصب از هسته)
ویندوز سرور	ویندوز سرور نسخه ۱۹۰۹(نصب از هسته)
ویندوز سرور	ویندوز سرور نسخه ۲۰۰۴(نصب از هسته)

منبع:

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/cve-2020-16898-bad-neighbor

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898