بسمه تعالی

انتشار وصله‌ی‌های امنیتی رایگان remote desktop مایکروسافت برای نسخه‌های قدیمی ویندوز جهت جلوگیری از بروز مجدد حملات WannaCry

مایکروسافت در به‌روزرسانی ماه می سال ۲۰۱۹ خود، ۷۹ آسیب‌پذیری از جمله یک آسیب‌پذیری در سیستم‌عامل‌های قدیمی Windows XP و Server 2003 که دیگر از آن‌ها پشتیبانی نمی‌کند را وصله کرده است.

معمولاً پشتیبانی از سیستم‌عامل‌های قدیمی هزینه‌بر است؛ اما مایکروسافت با توجه به ماهیت خطرناک این نقص بحرانی، وصله‌ی رایگانی را برای آن منتشر ساخته است. این آسیب‌پذیری با شناسه‌ی CVE-2019-0708 ردیابی می‌شود و در سرویس‌های Remote Desktop وجود دارد. این آسیب‌پذیری اجازه‌ی اجرای کد راه دور را می‌دهد؛ بدون آنکه نیازی به دخالت کاربر یا احرازهویت باشد. برای سوءاستفاده، مهاجم یکی از بیشمار بسته‌های ویندوزی آسیب‌پذیر را که به اینترنت یا یک شبکه متصل هستند را می‌یابد، بسته‌های ساختگی دقیق را به سرویس Remote Desktop آن ارسال می‌کند، اگر در حال اجرا باشد، شروع به اجرای کد مخرب در دستگاه می‌کند. از آنجا، رایانه‌های آسیب‌پذیر دیگر، با اسکن دامنه‌های IP، یافت خواهند شد. این آسیب‌پذیری «کرم‌گونه» است؛ بدین معنی که هر بدافزاری که در آینده از این آسیب‌پذیری سوءاستفاده می‌کند می‌تواند از رایانه‌ی آسیب‌پذیری به رایانه‌ی آسیب‌پذیر دیگر پخش شود. این روش مشابه روشی است که بدافزار WannaCry در سال ۲۰۱۷ در سراسر جهان انتشار یافت.

از آنجاییکه هیچ سوءاستفاده‌ای از این آسیب‌پذیری مشاهده نشده است، به احتمال زیاد، عاملین تهدید سوءاستفاده‌ای برای این آسیب‌پذیری خواهند نوشت و آن را در بدافزار خود قرار خواهند داد. لذا ضروری است سیستم‌های متأثر در اسرع وقت به‌منظور جلوگیری از چنین حوادثی، وصله شوند. به همین دلیل مایکروسافت به روزرسانی امنیتی برای تمامی مشتریان به‌منظور حفاظت بسترهای ویندوزی، از جمله برخی نسخه‌های قدیمی ویندوز ارایه کرده است. از آنجاییکه روش انتشار این آسیب‌پذیری ارزان قیمت و بسیار مؤثر برای اسپم‌کردن باج‌افزار و تروجان‌ها است، بدون شک به زودی چنین روش انتشار بدافزار مشاهده خواهد شد. Windows 8 و Windows 10 تحت‌تأثیر این آسیب‌پذیری قرار نگرفته‌اند. اما اگر نسخه‌های قدیمی‌تر وصله نشوند، تعداد زیادی از آن‌ها ممکن است آسیب ببینند. نسخه‌های ویندوزی متأثر این آسیب‌پذیری شامل Windows 7، Windows 2003، Windows Server 2008 R2، Windows Server 2008 و Windows XP هستند. با وصله‌کردن این آسیب‌پذیری، آسیب‌پذیری‌های زیاد دیگری نیز در به‌روزرسانی امنیتی ماه می سال ۲۰۱۹ مایکروسافت رفع شده‌اند.

از آسیب‌پذیری‌های وصله‌شده در این به‌روزرسانی، شش مورد از آن‌ها «بحرانی» و ۷۳ مورد «مهم» یا «پایین» رتبه‌بندی شده‌اند. این انتشار، همچنین شامل به‌روزرسانی‌هایی برای محصولات مختلف مایکروسافت مانند Internet Explorer، Edge، Office، سرویس‌ها و برنامه‌های کاربردی تحت وب Office، Azure DevOps Server، SQL Server، ChakraCore، NuGet، .NET Framework، .NET Core، Team Foundation Server، Visual Studio، Online Services و Skype برای ویندوز است.

آسیب‌پذیری CVE-2019-0863 (آسیب‌پذیری روز صفرم که به صورت گسترده‌ای مورد سوءاستفاده قرار گرفته است) در این به‌روزرسانی وصله شده است. این آسیب‌پذیری روز صفرم، یک آسیب‌پذیری افزایش امتیاز است که در روشی که سرویس گزارش‌دهی خطای ویندوز (WER) با فایل‌ها تعامل برقرار می‌کند، وجود دارد. این آسیب‌پذیری با شناسه‌ی CVE-2019-0863 ردیابی می‌شود. این آسیب‌پذیری توسط هکرها جهت افزایش دسترسی بر سیستم‌های در معرض خطر از یک حساب کاربری معمولی به حسابی با دسترسی مدیریتی به صورت گسترده‌ای مورد سوءاستفاده قرار گرفته است.

وصله‌ی امنیتی ماه می سال ۲۰۱۹ مایکروسافت، شامل یک وصله برای توصیه‌نامه‌ی ADV190013 نیز است. این توصیه‌نامه طرح مقابله‌ی مایکروسافت با مجموعه‌ی جدیدی از نقص‌های طراحی سخت‌افزاری CPU که به تازگی کشف شده‌اند را شرح می‌دهد (به نقص‌های امنیتی نمونه‌برداری داده‌های ریزمعماری (MDS) معروف است و اکثر CPUهای Intel منتشرشده در هشت سال گذشته را تحت‌تأثیر قرار می‌دهد). به گفته‌ی مایکروسافت، مشتریان به دو نوع به‌روزرسانی نیاز دارند. اولین به‌روزرسانی، به‌روزرسانی ریزکد سفت‌افزاری است که باید آن را از Intel یا OEMs خود (ارائه‌دندگان دستگاه) دریافت کنند. دومین به‌روزرسانی، به‌روزسانی امنیتی مایکروسافت است که برای هر دوی Windows و Windows Server منتشر ساخته است.

اطلاعات بیشتر در مورد به‌روزرسانی‌های ماه می سال ۲۰۱۹ مایکروسافت، در جدول زیر تعبیه شده است:

برچسب	شناسه CVE	عنوان CVE
به‌روزرسانی‌های پشته‌ی سرویس‌دهی (Servicing Stack)	ADV990001	آخرین به‌روزرسانی‌های پشته‌ی سرویس‌دهی

Adobe Flash Player	ADV190012	به‌روزرسانی امنیتی ماه می سال ۲۰۱۹ ادوبی
ویندوز مایکروسافت	ADV190013	راهنمای مایکروسافت جهت مقابله با آسیب‌پذیری‌های نمونه‌برداری داده‌های ریزمعماری (MDS)
.Net Core	CVE-2019-0982	آسیب‌پذیری انکار سرویس ASP.Net Core
.Net Core	CVE-2019-0981	آسیب‌پذیری انکار سرویس .Net Framework و .Net Core
.Net Core	CVE-2019-0980	آسیب‌پذیری انکار سرویس .Net Framework و .Net Core
.Net Framework	CVE-2019-0864	آسیب‌پذیری انکار سرویس .Net Framework
.Net Framework	CVE-2019-0820	آسیب‌پذیری انکار سرویس .Net Framework و .Net Core
Azure	CVE-2019-1000	آسیب‌پذیری افزایش امتیاز Azure AD Connect مایکروسافت
Internet Explorer	CVE-2019-0929	آسیب‌پذیری خرابی حافظه Internet Explorer
Internet Explorer	CVE-2019-0995	آسیب‌پذیری دورزدن ویژگی امنیتی Internet Explorer
Internet Explorer	CVE-2019-0930	آسیب‌پذیری افشای اطلاعات Internet Explorer
Internet Explorer	CVE-2019-0921	آسیب‌پذیری جاسوسی (Spoofing) Internet Explorer

Kerberos	CVE-2019-0734	آسیب‌پذیری افزایش امتیاز ویندوز
مرورگرهای مایکروسافت	CVE-2019-0940	آسیب‌پذیری خرابی حافظه مرورگر مایکروسافت
Microsoft Dynamics	CVE-2019-1008	آسیب‌پذیری دورزدن ویژگی امنیتی Microsoft Dynamics On-Permise
Microsoft Edge	CVE-2019-0938	آسیب‌پذیری افزایش امتیاز Microsoft Edge
Microsoft Edge	CVE-2019-0926	آسیب‌پذیری خرابی حافظه Microsoft Edge
Microsoft Graphics Component	CVE-2019-0892	آسیب‌پذیری افزایش امتیاز Win32k
Microsoft Graphics Component	CVE-2019-0961	آسیب‌پذیری افشای اطلاعات Windows GDI
Microsoft Graphics Component	CVE-2019-0758	آسیب‌پذیری افشای اطلاعات Windows GDI
Microsoft Graphics Component	CVE-2019-0903	آسیب‌پذیری اجرای کد راه‌دور GDI+
Microsoft Graphics Component	CVE-2019-0882	آسیب‌پذیری افشای اطلاعات Windows GDI
Microsoft JET Database Engine	CVE-2019-0898	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine
Microsoft JET Database Engine	CVE-2019-0895	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine
Microsoft JET Database Engine	CVE-2019-0897	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine
Microsoft JET Database Engine	CVE-2019-0889	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine
Microsoft JET Database Engine	CVE-2019-0890	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine

Microsoft JET Database Engine	CVE-2019-0891	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine
Microsoft JET Database Engine	CVE-2019-0896	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine
Microsoft JET Database Engine	CVE-2019-0893	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine
Microsoft JET Database Engine	CVE-2019-0894	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine
Microsoft JET Database Engine	CVE-2019-0901	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine
Microsoft JET Database Engine	CVE-2019-0899	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine
Microsoft JET Database Engine	CVE-2019-0900	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine
Microsoft JET Database Engine	CVE-2019-0902	آسیب‌پذیری اجرای کد راه‌دور Jet DataBase Engine
Microsoft Office	CVE-2019-0947	آسیب‌پذیری اجرای کد راه‌دور Microsoft Office Access Connectivity Engine
Microsoft Office	CVE-2019-0953	آسیب‌پذیری اجرای کد راه‌دور Microsoft Word
Microsoft Office	CVE-2019-0945	آسیب‌پذیری اجرای کد راه‌دور Microsoft Office Access Connectivity Engine
Microsoft Office	CVE-2019-0946	آسیب‌پذیری اجرای کد راه‌دور Microsoft Office Access Connectivity Engine
Microsoft Office SharePoint	CVE-2019-0957	آسیب‌پذیری افزایش امتیاز Microsoft SharePoint

Microsoft Office SharePoint	CVE-2019-0956	آسیب‌پذیری افشای اطلاعات Microsoft SharePoint Server
Microsoft Office SharePoint	CVE-2019-0949	آسیب‌پذیری جاسوسی Microsoft SharePoint
Microsoft Office SharePoint	CVE-2019-0950	آسیب‌پذیری جاسوسی Microsoft SharePoint
Microsoft Office SharePoint	CVE-2019-0952	آسیب‌پذیری اجرای کد راه‌دور Microsoft Office Server
Microsoft Office SharePoint	CVE-2019-0951	آسیب‌پذیری جاسوسی Microsoft SharePoint
Microsoft Office SharePoint	CVE-2019-0963	آسیب‌پذیری Microsoft Office XSS SharePoint
Microsoft Office SharePoint	CVE-2019-0958	آسیب‌پذیری افزایش امتیاز Microsoft SharePoint
Microsoft Scripting Engine	CVE-2019-0924	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine
Microsoft Scripting Engine	CVE-2019-0923	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine
Microsoft Scripting Engine	CVE-2019-0927	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine
Microsoft Scripting Engine	CVE-2019-0922	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine
Microsoft Scripting Engine	CVE-2019-0884	آسیب‌پذیری خرابی حافظه Scripting Engine
Microsoft Scripting Engine	CVE-2019-0933	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine
Microsoft Scripting Engine	CVE-2019-0925	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine

Microsoft Scripting Engine	CVE-2019-0937	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine
Microsoft Scripting Engine	CVE-2019-0918	آسیب‌پذیری خرابی حافظه Scripting Engine
Microsoft Scripting Engine	CVE-2019-0913	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine
Microsoft Scripting Engine	CVE-2019-0912	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine
Microsoft Scripting Engine	CVE-2019-0911	آسیب‌پذیری خرابی حافظه Scripting Engine
Microsoft Scripting Engine	CVE-2019-0914	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine
Microsoft Scripting Engine	CVE-2019-0917	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine
Microsoft Scripting Engine	CVE-2019-0916	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine
Microsoft Scripting Engine	CVE-2019-0915	آسیب‌پذیری خرابی حافظه Chakra Scripting Engine
Microsoft Windows	CVE-2019-0733	آسیب‌پذیری دورزدن ویژگی امنیتی Windows Defender Application Control
Microsoft Windows	CVE-2019-0936	آسیب‌پذیری افزایش امتیاز Windows
Microsoft Windows	CVE-2019-0886	آسیب‌پذیری افشای اطلاعات Windows Hyper-V
Microsoft Windows	CVE-2019-0863	آسیب‌پذیری افزایش امتیاز Windows Error Reporting
Microsoft Windows	CVE-2019-0942	آسیب‌پذیری افزایش امتیاز فیلترکردن نوشتن یکپارچه (Unified Write Filter)

Microsoft Windows	CVE-2019-0931	آسیب‌پذیری افزایش امتیاز Windows Storage Service
Microsoft Windows	CVE-2019-0885	آسیب‌پذیری اجرای کد راه‌دور Windows OLE
NuGet	CVE-2019-0976	آسیب‌پذیری دستکاری nugget Package Manager
Skype برای اندروید	CVE-2019-0932	آسیب‌پذیری افشای اطلاعات Skype برای اندروید
SQL Server	CVE-2019-0819	آسیب‌پذیری افشای اطلاعات Microsoft SQL Server Analysis Services
Team Foundation Server	CVE-2019-0971	آسیب‌پذیری افشای اطلاعات Azure DevOps Server و Team Foundation Server
Team Foundation Server	CVE-2019-0979	آسیب‌پذیری اسکریپت‌نویسی متقابل Azure DevOps Server و Team Foundation Server
Team Foundation Server	CVE-2019-0872	آسیب‌پذیری اسکریپت‌نویسی متقابل Azure DevOps Server و Team Foundation Server
Windows DHCP Server	CVE-2019-0725	آسیب‌پذیری اجرای کد راه‌دور Windows DHCP Server
Windows Diagnostic Hub	CVE-2019-0727	آسیب‌پذیری افزایش امتیاز Diagnostic Hub Standard Collector، Visual Studio Standard Collector
Windows Kernel	CVE-2019-0881	آسیب‌پذیری افزایش امتیاز Windows Kernel
Windows NDIS	CVE-2019-0707	آسیب‌پذیری افزایش امتیاز Windows

		NDIS
Windows RDP	CVE-2019-0708	آسیب‌پذیری اجرای کد راه‌دور Remote Desktop Services