بسمه‌تعالی

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر
مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای

گزارش آسیب‌پذیری Microsoft

گزارش فنی

شناسه سند ..... Microsoft_Vulnerability_Report
نوع سند ..... گزارش فنی
شماره نگارش ۱
تاریخ نگارش ۱۴۰۲/۰۳/۲۷
طبقه‌بندی سند ..... عادی

تهران، خیابان شهید بهشتی بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک۲۶۷
(۰۲۱) ۸۸۱۱۵۷۲۴ (۰۲۱) ۸۸۱۱۵۷۲۴ cert.ir

فهرست مطالب

۱ شرح آسیب‌پذیری

مایکروسافت در به‌روزرسانی‌های امنیتی (ژوئن ۲۰۲۳) ۷۸ آسیب‌پذیری را گزارش داده است. طبقه بندی آسیب‌پذیری‌ها به شرح زیر است:

- افزایش سطح دسترسی : ۱۷
- عبور از ویژگی‌های امنیتی: ۳
- اجرای کد از راه دور: ۳۲
- افشای اطلاعات: ۵
- منع از سرویس (Denial of Service): ۱۰
- سوءاستفاده از هویت: ۱۰
- آسیب‌پذیری مربوط به Edge – Chromium : ۱ مورد

شش مورد از این ۷۸ آسیب پذیری ، بحرانی طبقه بندی شدند و امکان اجرای کد از راه دور و افزایش امتیاز را می‌دهند و بقیه هم با شدت بالا، متوسط و شدت پایین تعریف شده‌اند. در این بروزرسانی زیرودی یا آسیب پذیری که از قبل اکسپلویت شده باشد وجود ندارد و فقط آسیب پذیری Chromium قبلا اکسپلویت شده است.

آسیب پذیری CVE-2023-29357 :

آسیب‌پذیری در Microsoft SharePoint Server است و با شدت بحرانی و امتیاز ۹,۸ را دارا است. مهاجم با بدست آوردن توکن های جعلی JWT ، می‌تواند با این آسیب‌پذیری امتیاز خود را به کاربر Administrator افزایش دهد. آسیب پذیری در جریان مسابقات Pwn2Own Vancouver کشف و گزارش شده است. آسیب پذیری به دلیل نقص در متد ValidateTokenIssuer رخ میدهد که امکان دور زدن احرازهویت را فراهم میکند. برای اکسپلویت نیاز به تعامل کاربر یا امتیاز خاص نیست و پیچیدگی کمی هم دارد مایکروسافت اعلام کرده است اگر امکان بروزرسانی را ندارید، مشتریانی که از دیفندر ویندوز و AMSI استفاده می‌کنند در برابر این آسیب پذیری امن هستند.

نسخه تحت تاثیر :
Microsoft SharePoint Server 2019

آسیب پذیری CVE-2023-29363 و CVE-2023-32015 و CVE-2023-32014 :

آسیب پذیری در Windows Pragmatic General Multicast (PGM) است. آسیب پذیری با شدت بحرانی و امتیاز ۹,۸ است. اگر سرویس Windows message queuing در PGM Server در حال اجرا باشد، مهاجم بدون احرازهویت میتواند با ارسال یک فایل مخرب ، به اجرای کد از راه دور دست پیدا کند. نکته مهم این است که این سومین ماهی است که PGM یک آسیب پذیری با امتیاز ۹,۸ می‌دهد، بنابراین میتواند یک منطقه کاندید برای کشف آسیب پذیری باشد. البته PGM بطور پیش فرض فعال نیست . برای اینکه تحت تاثیر آسیب پذیری واقع شوید باید Windows message queuing فعال باشد و همچنین برای چک کردن آن ، این سرویس روی پورت TCP 1801 فعال است.

نسخه های تحت تاثیر :
Windows Server 2012 R2
Windows Server 2012
Windows Server 2008 R2
Windows Server 2008
Windows Server 2016
Windows 10 Version 1607
Windows 10
Windows 10 Version 22H2
Windows 11 Version 22H2
Windows 10 Version 21H2
Windows 11 Version 21H2
Windows Server 2022
Windows Server 2019
Windows 10 Version 1809

آسیب پذیری CVE-2023-24897 :

آسیب پذیری در .NET و .NET Framework و Visual Studio است. این آسیب پذیری دارای شدت بحرانی و امتیاز ۷,۳ است و امکان اجرای کد دلخواه را می‌دهد. این آسیب پذیری از نوع ACE است (اجرای کد دلخواه بصورت محلی). در واقع مهاجم باید قربانی رو فریب دهد تا یک فایل مخربی رو دانلود و اجرا کند. برای اکسپلویت پیچیدگی کم و نیاز به تعامل کاربر دارد و همچنین امتیاز خاصی هم نیاز ندارد.

نسخه های تحت تاثیر :
Microsoft .NET Framework 3.5
Microsoft .NET Framework 4.8
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.8.1
Microsoft .NET Framework 4.7
Microsoft .NET Framework 4.7.2
Microsoft .NET Framework 4.7.1
Microsoft Visual Studio 2022 version 17.6
.NET 6.0
.NET 7.0
Microsoft Visual Studio 2013 Update 5
Microsoft Visual Studio 2022 version 17.4
Microsoft Visual Studio 2022 version 17.0
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10(
Microsoft Visual Studio 2022 version 17.2
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 – 15.8(

آسیب پذیری آسیب پذیری CVE-2023-32013 :

این آسیب پذیری در Windows Hyper-V است و امتیاز ۶,۵ را دارد. آسیب پذیری امکان DoS رو میدهد اما برای اکسپلویت نیاز به شرایطی است که باید در محیط قربانی فراهم شود.

نسخه های تحت تاثیر :
Windows 10 Version 22H2
Windows 11 Version 22H2
Windows 10 Version 21H2
Windows 11 Version 21H2
Windows Server 2022
Windows Server 2019
Windows 10 Version 1809

آسیب پذیری CVE-2023-32031:

آسیب پذیری در Microsoft Exchange Server و دارای امتیاز ۸,۸ است. این آسیب پذیری یک روش دور زدن برای آسیب پذیری های اصلاح شده CVE-2022-41082 و CVE-2023-21529 است. آسیب پذیری در کلاس Command و از نوع Deserialization است. برای اکسپلویت، مهاجم باید احرازهویت شود، اما اکسپلویت موفق امکان اجرای کد با امتیاز SYSTEM رو میدهد.

نسخه های تحت تاثیر :
Microsoft Exchange Server 2019 Cumulative Update 13
Microsoft Exchange Server 2016 Cumulative Update 23
Microsoft Exchange Server 2019 Cumulative Update 12

آسیب پذیری CVE-2023-28310:

آسیب پذیری در Microsoft Exchange Server و دارای امتیاز ۸,۰ است. مهاجم امکان اجرای کد را دارد و برای اکسپلویت، مهاجم باید احرازهویت شود. اما اکسپلویت موفق امکان اجرای کد با امتیاز SYSTEM رو میدهد.

نسخه های تحت تاثیر :
Microsoft Exchange Server 2019 Cumulative Update 13
Microsoft Exchange Server 2016 Cumulative Update 23
Microsoft Exchange Server 2019 Cumulative Update 12

آسیب پذیری CVE-2023-32029 و CVE-2023-33133 و CVE-2023-33137 :

آسیب پذیری در Microsoft Excel و دارای امتیاز ۷٫۸ و شدت مهم است. مهاجم با ارسال یک فایل مخرب ، میتواند کد دلخواه اجرا خود را اجرا کند. این آسیب پذیری از نوع ACE است.

نسخه های تحت تاثیر :
Microsoft Excel 2013 Service Pack 1
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2016
Microsoft Office LTSC 2021
Microsoft Office LTSC for Mac 2021
Microsoft 365 Apps for Enterprise
Microsoft Office Online Server
Microsoft Office 2019 for Mac
Microsoft Office 2019

آسیب پذیری CVE-2023-33146 :

آسیب پذیری در Microsoft Office است و امکان اجرای کد را به مهاجم می‌دهد. دارای امتیاز ۸.۷ و شدت مهم است. مهاجم با ارسال یک فایل مخرب و فریب کاربر برای باز کردن فایل، از این آسیب پذیری سوء استفاده می‌کند.

نسخه های تحت تاثیر :
Microsoft Office LTSC for Mac 2021
Microsoft 365 Apps for Enterprise
Microsoft Office 2019 for Mac

آسیب پذیری CVE-2023-29362 :

این آسیب پذیری در قسمت Remote Desktop Client است و دارای شدت مهم و امتیاز ۸٫۸ است. مهاجم باید یک سرور مخرب Remote Desktop Server داشته باشد، زمانی کلاینت به آن وصل شد، امکان اجرای کد دلخواه را دارد.

نسخه های تحت تاثیر :
Windows Server 2012 R2
Windows Server 2012
Windows Server 2008 R2
Windows Server 2016
Windows 10 Version 1607
Windows 10
Windows 10 Version 22H2
Windows 11 Version 22H2
Windows 10 Version 21H2
Windows 11 Version 21H2
Windows Server 2022
Remote Desktop client for Windows Desktop
Windows Server 2019
Windows 10 Version 1809

آسیب پذیری CVE-2023-3079 :

آسیب پذیری در Chromium و با توجه به اینکه Microsoft Edge مبتنی بر Chromium است، تحت تاثیر این آسیب پذیری قرار میگیرد. آسیب پذیری از نوع Type Confusion در V8 است. این آسیب پذیری در حملاتی مورد اکسپلویت قرار گرفته است.

۲ مراجع

https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2023-patch-tuesday-fixes-78-flaws-38-rce-bugs/