MICROSOFT CORRIGE 118 VULNERABILIDADES, INCLUIDAS 5 VULNERABILIDADES DE ZERO DAY EN LA ACTUALIZACION DE SEGURIDAD DE OCTUBRE

Recientemente, Microsoft corrigió 118 vulnerabilidades en su martes de actualizaciones de OCT24, incluyendo 5 zero day.

El Patch Tuesday de OCT24 de Microsoft, se lanzaron actualizaciones de seguridad que abordan 118 vulnerabilidades, incluidas cinco vulnerabilidades de tipo zero-day, dos de las cuales ya estaban siendo activamente explotadas. Entre estas vulnerabilidades, tres son críticas y están relacionadas con la ejecución remota de código (RCE).

Las vulnerabilidades corregidas se dividen en las siguientes categorías:

- 28 de elevación de privilegios,
- 7 de omisión de características de seguridad,
- 43 de ejecución remota de código,
- 6 de divulgación de información,
- 26 de denegación de servicio y
- 7 de suplantación.

Además, el recuento no incluye tres fallos en Microsoft Edge que fueron corregidos previamente el 3OCT24.

Detalles de los zero-days:

De los cinco zero-days corregidos este mes, dos estaban siendo activamente explotados:

- **CVE-2024-43573:** Vulnerabilidad de suplantación en la plataforma MSHTML de Windows. Aunque Microsoft no ha compartido muchos detalles sobre este fallo, se sabe que está relacionado con la plataforma MSHTML, que fue utilizada por Internet Explorer y Edge Legacy. A pesar de que ambas aplicaciones están retiradas, los componentes subyacentes de MSHTML siguen presentes en Windows. Se especula que esta vulnerabilidad podría estar relacionada con un fallo anterior que permitía la suplantación de extensiones de archivos.
- **CVE-2024-43572:** Vulnerabilidad de ejecución remota de código en la Consola de Administración de Microsoft (MMC). Esta vulnerabilidad permitía a archivos de consola guardados (.MSC) ejecutar código remoto en dispositivos vulnerables. Microsoft corrigió el fallo impidiendo la apertura de archivos MSC no confiables.

Los otros tres zero-days que fueron divulgados públicamente pero no explotados activamente son:

- **CVE-2024-6197:** Vulnerabilidad de ejecución remota de código en Curl. Se corrigió un fallo en la librería libcurl que podría permitir la ejecución de

comandos cuando Curl intenta conectarse a un servidor malicioso con un certificado TLS manipulado.

- **CVE-2024-20659:** Vulnerabilidad de omisión de características de seguridad en Hyper-V. Este fallo permitía a los atacantes comprometer el hipervisor y el kernel mediante la omisión del firmware UEFI en algunos equipos. Requiere acceso físico al dispositivo.
- **CVE-2024-43583:** Vulnerabilidad de elevación de privilegios en Winlogon. Este fallo permitía que un atacante obtuviera privilegios de SYSTEM. Para estar completamente protegidos, los administradores deben habilitar un IME de primera parte de Microsoft para evitar posibles vulnerabilidades asociadas con IMEs de terceros durante el proceso de inicio de sesión.

A continuación, se presenta la lista completa de vulnerabilidades corregidas en las actualizaciones de seguridad correspondientes al Patch Tuesday de OCT24.

Tag	CVE ID	CVE Title	Severity
.NET and Visual Studio	CVE-2024-38229	.NET and Visual Studio Remote Code Execution Vulnerability	Important
.NET and Visual Studio	CVE-2024-43485	.NET and Visual Studio Denial of Service Vulnerability	Important
.NET, .NET Framework, Visual Studio	CVE-2024-43484	.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability	Important
.NET, .NET Framework, Visual Studio	CVE-2024-43483	.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability	Important
Azure CLI	CVE-2024-43591	Azure Command Line Integration (CLI) Elevation of Privilege Vulnerability	Important
Azure Monitor	CVE-2024-38097	Azure Monitor Agent Elevation of Privilege Vulnerability	Important
Azure Stack	CVE-2024-38179	Azure Stack Hyperconverged Infrastructure (HCI) Elevation of Privilege Vulnerability	Important
BranchCache	CVE-2024-43506	BranchCache Denial of Service Vulnerability	Important
BranchCache	CVE-2024-38149	BranchCache Denial of Service Vulnerability	Important
Code Integrity Guard	CVE-2024-43585	Code Integrity Guard Security Feature Bypass Vulnerability	Important

DeepSpeed	CVE-2024-43497	DeepSpeed Remote Code Execution Vulnerability	Important
Internet Small Computer Systems Interface (iSCSI)	CVE-2024-43515	Internet Small Computer Systems Interface (iSCSI) Denial of Service Vulnerability	Important
Microsoft ActiveX	CVE-2024-43517	Microsoft ActiveX Data Objects Remote Code Execution Vulnerability	Important
Microsoft Configuration Manager	CVE-2024-43468	Microsoft Configuration Manager Remote Code Execution Vulnerability	**Critical**
Microsoft Defender for Endpoint	CVE-2024-43614	Microsoft Defender for Endpoint for Linux Spoofing Vulnerability	Important
Microsoft Edge (Chromium-based)	CVE-2024-9369	Chromium: CVE-2024-9369 Insufficient data validation in Mojo	Unknown
Microsoft Edge (Chromium-based)	CVE-2024-9370	Chromium: CVE-2024-9370 Inappropriate implementation in V8	Unknown
Microsoft Edge (Chromium-based)	CVE-2024-7025	Chromium: CVE-2024-7025 Integer overflow in Layout	Unknown
Microsoft Graphics Component	CVE-2024-43534	Windows Graphics Component Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2024-43508	Windows Graphics Component Information Disclosure Vulnerability	Important
Microsoft Graphics Component	CVE-2024-43556	Windows Graphics Component Elevation of Privilege Vulnerability	Important
Microsoft Graphics Component	CVE-2024-43509	Windows Graphics Component Elevation of Privilege Vulnerability	Important
Microsoft Management Console	CVE-2024-43572	Microsoft Management Console Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2024-43616	Microsoft Office Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2024-43576	Microsoft Office Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2024-43609	Microsoft Office Spoofing Vulnerability	Important

Microsoft Office Excel	CVE-2024-43504	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office SharePoint	CVE-2024-43503	Microsoft SharePoint Elevation of Privilege Vulnerability	Important
Microsoft Office Visio	CVE-2024-43505	Microsoft Office Visio Remote Code Execution Vulnerability	Important
Microsoft Simple Certificate Enrollment Protocol	CVE-2024-43544	Microsoft Simple Certificate Enrollment Protocol Denial of Service Vulnerability	Important
Microsoft Simple Certificate Enrollment Protocol	CVE-2024-43541	Microsoft Simple Certificate Enrollment Protocol Denial of Service Vulnerability	Important
Microsoft WDAC OLE DB provider for SQL	CVE-2024-43519	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	Important
Microsoft Windows Speech	CVE-2024-43574	Microsoft Speech Application Programming Interface (SAPI) Remote Code Execution Vulnerability	Important
OpenSSH for Windows	CVE-2024-43615	Microsoft OpenSSH for Windows Remote Code Execution Vulnerability	Important
OpenSSH for Windows	CVE-2024-43581	Microsoft OpenSSH for Windows Remote Code Execution Vulnerability	Important
OpenSSH for Windows	CVE-2024-38029	Microsoft OpenSSH for Windows Remote Code Execution Vulnerability	Important
Outlook for Android	CVE-2024-43604	Outlook for Android Elevation of Privilege Vulnerability	Important
Power BI	CVE-2024-43612	Power BI Report Server Spoofing Vulnerability	Important
Power BI	CVE-2024-43481	Power BI Report Server Spoofing Vulnerability	Important
Remote Desktop Client	CVE-2024-43533	Remote Desktop Client Remote Code Execution Vulnerability	Important
Remote Desktop Client	CVE-2024-43599	Remote Desktop Client Remote Code Execution Vulnerability	Important
Role: Windows Hyper-V	CVE-2024-43521	Windows Hyper-V Denial of Service Vulnerability	Important

Role: Windows Hyper-V	CVE-2024-20659	Windows Hyper-V Security Feature Bypass Vulnerability	Important
Role: Windows Hyper-V	CVE-2024-43567	Windows Hyper-V Denial of Service Vulnerability	Important
Role: Windows Hyper-V	CVE-2024-43575	Windows Hyper-V Denial of Service Vulnerability	Important
RPC Endpoint Mapper Service	CVE-2024-43532	Remote Registry Service Elevation of Privilege Vulnerability	Important
Service Fabric	CVE-2024-43480	Azure Service Fabric for Linux Remote Code Execution Vulnerability	Important
Sudo for Windows	CVE-2024-43571	Sudo for Windows Spoofing Vulnerability	Important
Visual C++ Redistributable Installer	CVE-2024-43590	Visual C++ Redistributable Installer Elevation of Privilege Vulnerability	Important
Visual Studio	CVE-2024-43603	Visual Studio Collector Service Denial of Service Vulnerability	Important
Visual Studio Code	CVE-2024-43488	Visual Studio Code extension for Arduino Remote Code Execution Vulnerability	**Critical**
Visual Studio Code	CVE-2024-43601	Visual Studio Code for Linux Remote Code Execution Vulnerability	Important
Windows Ancillary Function Driver for WinSock	CVE-2024-43563	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Important
Windows BitLocker			