e-dea NETWORKS | CYBER SECURITY

BOLETÍN
INFORMATIVO

24 – Marzo – 2026

Vulnerabilidades en Microsoft

Detalles

Microsoft ha lanzado actualizaciones de seguridad que cubren 110 vulnerabilidades con CVE asignado. De ellas, 79 tienen una calificación de riesgo alto y 31 de riesgo medio.

Estas vulnerabilidades permiten a atacantes obtener permisos, ejecutar código, obtener información sensible, evadir características de seguridad y ataques de denegación de servicio.

La CVE-2026-21316, que afecta a Microsoft Streaming Service, está siendo explotada activamente.

Boletín Informativo

Productos afectados

Producto afectado	CVE	Base Score	Producto afectado	CVE	Base Score	Producto afectado	CVE	Base Score
Microsoft Edge for Android	CVE-2026-0385	5	Push Message Routing Service	CVE-2026-24282	5.5	Windows Authentication Methods	CVE-2026-25171	7
System Center Operations Manager	CVE-2026-20967	8.8	Windows File Server	CVE-2026-24283	8.8	Windows Routing and Remote Access Service (RRAS)	CVE-2026-25172	8
SQL Server	CVE-2026-21262	8.8	Windows Win32K	CVE-2026-24285	7	Windows Routing and Remote Access Service (RRAS)	CVE-2026-25173	8
Microsoft Devices Pricing Program	CVE-2026-21536	9.8	Windows Kernel	CVE-2026-24287	7.8	Windows Extensible File Allocation	CVE-2026-25174	7.8
Azure Compute Gallery	CVE-2026-23651	6.7	Windows Mobile Broadband	CVE-2026-24288	6.8	Windows NTFS	CVE-2026-25175	7.8
GitHub Repo: zero-shot-scfoundation	CVE-2026-23654	8.8	Windows Kernel	CVE-2026-24289	7.8	Windows Ancillary Function Driver for WinSock	CVE-2026-25176	7.8
Windows App Installer	CVE-2026-23656	5.9	Windows Projected File System	CVE-2026-24290	7.8	Active Directory Domain Services	CVE-2026-25177	8.8
Azure DevOps	CVE-2026-23658	8.6	Windows Accessibility Infrastructure (ATBroker.exe)	CVE-2026-24291	7.8	Windows Ancillary Function Driver for WinSock	CVE-2026-25178	7
Azure Data Factory	CVE-2026-23659	8.6	Connected Devices Platform Service (Cdpsvc)	CVE-2026-24292	7.8	Windows Ancillary Function Driver for WinSock	CVE-2026-25179	7
Azure Portal Windows Admin Center	CVE-2026-23660	7.8	Windows Ancillary Function Driver for WinSock	CVE-2026-24293	7.8	Microsoft Graphics Component	CVE-2026-25180	5.5
Azure IoT Explorer	CVE-2026-23661	7.5	Windows SMB Server	CVE-2026-24294	7.8	Windows GDI+	CVE-2026-25181	7.5
Azure IoT Explorer	CVE-2026-23662	7.5	Windows Device Association Service	CVE-2026-24295	7	Windows Shell Link Processing	CVE-2026-25185	5.3
Azure IoT Explorer	CVE-2026-23664	7.5	Windows Device Association Service	CVE-2026-24296	7	Windows Accessibility Infrastructure (ATBroker.exe)	CVE-2026-25186	5.5
Azure Linux Virtual Machines	CVE-2026-23665	7.8	Windows Kerberos	CVE-2026-24297	6.5	Winlogon	CVE-2026-25187	7.8
Broadcast DVR	CVE-2026-23667	7	M365 Copilot	CVE-2026-24299	5.3	Windows Telephony Service	CVE-2026-25188	8.8
Microsoft Graphics Component	CVE-2026-23668	7	Windows Performance Counters	CVE-2026-25165	7.8	Windows DWM Core Library	CVE-2026-25189	7.8
Windows Print Spooler Components	CVE-2026-23669	8.8	Windows System Image Manager	CVE-2026-25166	7.8	Windows GDI	CVE-2026-25190	7.8
Windows Bluetooth RFCOM Protocol Driver	CVE-2026-23671	7	Microsoft Brokering File System	CVE-2026-25167	7.4	Microsoft Office SharePoint	CVE-2026-26105	8.1
Windows Universal Disk Format File System Driver (UDFS)	CVE-2026-23672	7.8	Microsoft Graphics Component	CVE-2026-25168	6.2	Microsoft Office SharePoint	CVE-2026-26106	8.8
Windows Resilient File System (ReFS)	CVE-2026-23673	7.8	Microsoft Graphics Component	CVE-2026-25169	6.2	Microsoft Office Excel	CVE-2026-26107	7.8
Windows MapUrlToZone	CVE-2026-23674	7.5	Role: Windows Hyper-V	CVE-2026-25170	7	Microsoft Office Excel	CVE-2026-26108	7.8
Microsoft Office Excel	CVE-2026-26112	7.8	Windows Kernel	CVE-2026-26132	7.8	Microsoft Office Excel	CVE-2026-26109	8.4
Microsoft Office	CVE-2026-26113	8.4	M365 Copilot	CVE-2026-26133	7.1	Microsoft Office	CVE-2026-26110	8.4
Microsoft Office SharePoint	CVE-2026-26114	8.8	Microsoft Office	CVE-2026-26134	7.8	Windows Routing and Remote Access Service (RRAS)	CVE-2026-26111	8
SQL Server	CVE-2026-26115	8.8	Microsoft Copilot	CVE-2026-26136	6.5	.NET	CVE-2026-26127	7.5
SQL Server	CVE-2026-26116	8.8	Microsoft 365 Copilot's Business Chat	CVE-2026-26137	8.9	Windows SMB Server	CVE-2026-26128	7.8
Azure Windows Virtual Machine Agent	CVE-2026-26117	7.8	Microsoft Purview	CVE-2026-26138	8.6	ASP.NET Core	CVE-2026-26130	7.5
Azure MCP Server	CVE-2026-26118	8.8	Microsoft Purview	CVE-2026-26139	8.6	.NET	CVE-2026-26131	7.8
Microsoft Bing	CVE-2026-26120	6.5	Azure Arc	CVE-2026-26141	7.8	Azure Compute Gallery	CVE-2026-26124	6.7
Azure IoT Explorer	CVE-2026-26121	7.5	Microsoft Office Excel	CVE-2026-26144	7.5	Payment Orchestrator Service	CVE-2026-26125	8.6
Azure Compute Gallery	CVE-2026-26122	6.5	Azure Entra ID	CVE-2026-26148	8.1	Microsoft Bing Images	CVE-2026-32191	9.8
Microsoft Authenticator	CVE-2026-26123	5.5	Azure Cloud Shell	CVE-2026-32169	10	Microsoft Bing Images	CVE-2026-32194	9.8

Recomendaciones

Priorizar el parche "Zero-Day": Centra los esfuerzos iniciales en la actualización de Microsoft Streaming Service, ya que la vulnerabilidad CVE-2026-21316 está siendo utilizada en ataques reales.

Ciclo de Actualización Crítico: Configurar los sistemas críticos para recibir las actualizaciones de seguridad de marzo de 2026 mediante Windows Update o WSUS lo antes posible.

Fuentes: Microsoft