e-dea NETWORKS | CYBER SECURITY



BOLETÍN
INFORMATIVO

14 - octubre – 2026

Vulnerabilidades críticas en Microsoft

Microsoft publicó actualizaciones de seguridad para octubre de 2026.

De las vulnerabilidades encontradas, Microsoft clasifica como críticos: 65 de ejecución remota de código, 11 de elevación de privilegios y 2 de suplantación de identidad.

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-97814	Windows Text Shaping	Ejecución remota de código	9.8	Crítica
CVE-2026-97780	Microsoft Office Excel	Ejecución remota de código	8.8	Crítica
CVE-2026-97778	Microsoft Office Excel	Ejecución remota de código	8.8	Crítica
CVE-2026-97776	Microsoft Office Excel	Ejecución remota de código	8.8	Alta
CVE-2026-97767	Microsoft Office Excel	Ejecución remota de código	8.8	Alta

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-97765	Microsoft Office Excel	Ejecución remota de código	8.8	Crítica
CVE-2026-97761	Microsoft Office Excel	Ejecución remota de código	8.8	Alta
CVE-2026-97759	Microsoft Office Excel	Ejecución remota de código	8.8	Crítica
CVE-2026-97758	Microsoft Office Excel	Ejecución remota de código	8.8	Alta
CVE-2026-97756	Microsoft Office Excel	Ejecución remota de código	8.8	Alta

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-97755	Microsoft Office Excel	Ejecución remota de código	8.8	Crítica
CVE-2026-97753	Microsoft Office Excel	Ejecución remota de código	8.8	Alta
CVE-2026-97749	Microsoft Office Outlook	Ejecución remota de código	9.8	Crítica
CVE-2026-97745	Microsoft Office Excel	Ejecución remota de código	8.8	Crítica
CVE-2026-97742	Microsoft Office Excel	Ejecución remota de código	8.8	Alta

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-97741	Microsoft Office Excel	Ejecución remota de código	8.8	Alta
CVE-2026-97739	Microsoft Office Excel	Ejecución remota de código	8.8	Crítica
CVE-2026-97016	Microsoft Office Outlook	Ejecución remota de código	9.8	Crítica
CVE-2026-96952	Microsoft Windows Media Foundation	Ejecución remota de código	8.8	Crítica
CVE-2026-96943	Windows Raw Image Extension	Ejecución remota de código	8.8	Crítica

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-96934	Windows DHCP Server	Ejecución remota de código	9.8	Crítica
CVE-2026-96914	Windows Virtualization-Based Security (VBS) Enclave	Elevación de privilegios	8.8	Crítica
CVE-2026-96913	Windows Kernel	Elevación de privilegios	8.8	Crítica
CVE-2026-96222	Active Directory Federation Services (AD FS)	Suplantación de identidad	7.4	Crítica
CVE-2026-96202	Windows Raw Image Extension	Ejecución remota de código	8.8	Crítica

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-88207	Microsoft Office PowerPoint	Ejecución remota de código	7.5	Alta
CVE-2026-88185	Microsoft Office Word	Ejecución remota de código	8.1	Crítica
CVE-2026-88178	Microsoft Office PowerPoint	Ejecución remota de código	9.8	Crítica
CVE-2026-88174	Windows Deployment Services	Ejecución remota de código	8.1	Crítica
CVE-2026-88171	Windows DHCP Server	Ejecución remota de código	8.1	Crítica

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-88156	Microsoft Office Outlook	Ejecución remota de código	9.8	Crítica
CVE-2026-88144	Microsoft Office PowerPoint	Ejecución remota de código	8.8	Crítica
CVE-2026-88120	Windows DHCP Server	Ejecución remota de código	8.1	Crítica
CVE-2026-88119	Windows DHCP Server	Ejecución remota de código	8.1	Crítica
CVE-2026-88117	Windows DHCP Server	Ejecución remota de código	8.1	Crítica

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-88074	Windows Virtualization-Based Security (VBS) Enclave	Elevación de privilegios	7.8	Crítica
CVE-2026-88073	Windows Graphics Kernel	Elevación de privilegios	8.8	Crítica
CVE-2026-83934	Windows GDI+	Ejecución remota de código	8.8	Crítica
CVE-2026-83917	Windows ALPC	Elevación de privilegios	7.0	Crítica
CVE-2026-70571	Microsoft Exchange Server	Ejecución remota de código	8.1	Crítica

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-70300	Microsoft Office Word	Ejecución remota de código	9.8	Alta
CVE-2026-70291	Microsoft Office Outlook	Ejecución remota de código	9.8	Crítica
CVE-2026-70269	Microsoft Office Word	Ejecución remota de código	8.1	Crítica
CVE-2026-70250	Windows DHCP Client	Ejecución remota de código	8.8	Crítica
CVE-2026-70242	Microsoft Office Outlook	Ejecución remota de código	9.8	Crítica

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-70229	Active Directory Domain Services	Ejecución remota de código	8.1	Crítica
CVE-2026-70215	Microsoft Office PowerPoint	Ejecución remota de código	8.8	Crítica
CVE-2026-70187	Remote Desktop Gateway Service	Ejecución remota de código	8.1	Crítica
CVE-2026-70153	Microsoft PostScript Printer Driver	Ejecución remota de código	9.8	Crítica
CVE-2026-70147	Microsoft PostScript Printer Driver	Ejecución remota de código	9.8	Crítica

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-69802	Network Device Enrollment Service (NDES)	Ejecución remota de código	8.1	Crítica
CVE-2026-69789	Reliable Multicast Transport Driver (RMCAST)	Ejecución remota de código	7.5	Crítica
CVE-2026-62840	Linux Kernel	Elevación de privilegios	7.0	Crítica
CVE-2026-108471	Windows Virtualization-Based Security (VBS) Enclave	Elevación de privilegios	8.8	Crítica
CVE-2026-108467	Microsoft PostScript Printer Driver	Ejecución remota de código	8.8	Crítica

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-108460	Windows Message Queuing	Ejecución remota de código	8.1	Crítica
CVE-2026-108457	Microsoft Windows PDF	Ejecución remota de código	8.1	Crítica
CVE-2026-108400	Microsoft Windows Codecs Library	Ejecución remota de código	8.8	Crítica
CVE-2026-108399	Windows Hyper-V	Elevación de privilegios	7.2	Crítica
CVE-2026-108131	Active Directory Federation Services (AD FS)	Suplantación de identidad	7.5	Crítica

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-108130	Windows Virtualization-Based Security (VBS) Enclave	Elevación de privilegios	7.8	Crítica
CVE-2026-105733	Windows Hyper-V	Ejecución remota de código	8.8	Crítica
CVE-2026-105718	Microsoft Office Excel	Ejecución remota de código	8.8	Crítica
CVE-2026-105016	Microsoft QUIC	Ejecución remota de código	9.8	Crítica
CVE-2026-102866	Microsoft Office SharePoint	Elevación de privilegios	8.1	Crítica

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-102857	Microsoft Office Visio	Ejecución remota de código	8.8	Crítica
CVE-2026-102856	Microsoft Office Visio	Ejecución remota de código	8.8	Crítica
CVE-2026-102855	Microsoft Office Visio	Ejecución remota de código	8.8	Crítica
CVE-2026-102225	Windows Text Shaping	Ejecución remota de código	8.8	Crítica
CVE-2026-102214	Windows Hyper-V	Ejecución remota de código	8.8	Crítica

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-102211	Windows Virtualization-Based Security (VBS) Enclave	Elevación de privilegios	7.0	Crítica
CVE-2026-100220	Windows Media Video Decoder	Ejecución remota de código	8.8	Crítica
CVE-2026-100219	Microsoft QUIC	Ejecución remota de código	9.8	Crítica
CVE-2026-100215	Microsoft Graphics Component	Ejecución remota de código	7.8	Crítica
CVE-2026-100211	Microsoft Office Excel	Ejecución remota de código	8.8	Crítica

Vulnerabilidades **críticas**

CVE	Producto / componente	Impacto	CVSS	MSRC
CVE-2026-100210	Microsoft Office Excel	Ejecución remota de código	8.8	Crítica
CVE-2026-100209	Microsoft Office Excel	Ejecución remota de código	8.8	Crítica
CVE-2026-100202	Windows Message Queuing Queue Manager	Ejecución remota de código	9.8	Crítica

Recomendaciones



Severidad: **Crítica**

Parches

Instalar las actualizaciones de octubre mediante Windows Update, Microsoft Update.

Validación

- *Consultar en MSRC los parches aplicables a cada producto y versión.*
- *INCIBE recomienda priorizar CVE-2026-96951 por explotación activa.*

Fuentes: INCIBE-CERT y Microsoft MSRC