CYBER SECURITY

BOLETÍN INFORMATIVO

11 – Diciembre - 2024

Vulnerabilidades en Microsoft

Detalles:

El fabricante Microsoft emite comunicado sobre la corrección de 71 vulnerabilidades que afectan a diferentes productos.

e-dea NETWORKS

CVE's de Severidad Crítica y Alta:

CVE	CVSS	Tipo de vulnerabilidad
CVE-2024-49112	9.8	Vulnerabilidad de ejecución remota de código en el Protocolo ligero de acceso a directorios (LDAP) de Windows
CVE-2024-49117	8.8	Vulnerabilidad de ejecución remota de código en Windows Hyper-V
CVE-2024-49124	8.1	Vulnerabilidad de ejecución remota de código en el cliente del Protocolo ligero de acceso a directorios (LDAP)
CVE-2024-49127	8.1	Vulnerabilidad de ejecución remota de código en el Protocolo ligero de acceso a directorios (LDAP) de Windows
CVE-2024-49126	8.1	Vulnerabilidad de ejecución remota de código en el servicio de subsistema de autoridad de seguridad local (LSASS) de Windows
CVE-2024-49118	8.1	Vulnerabilidad de ejecución remota de código en Microsoft Message Queue (MSMQ)
CVE-2024-49122	8.1	Vulnerabilidad de ejecución remota de código en Microsoft Message Queue (MSMQ)
CVE-2024-49132	8.1	Vulnerabilidad de ejecución remota de código en los Servicios de Escritorio Remoto de Windows
CVE-2024-49115	8.1	Vulnerabilidad de ejecución remota de código en los Servicios de Escritorio Remoto de Windows
CVE-2024-49116	8.1	Vulnerabilidad de ejecución remota de código en los Servicios de Escritorio Remoto de Windows
CVE-2024-49123	8.1	Vulnerabilidad de ejecución remota de código en los Servicios de Escritorio Remoto de Windows
CVE-2024-49128	8.1	Vulnerabilidad de ejecución remota de código en los Servicios de Escritorio Remoto de Windows
CVE-2024-49106	8.1	Vulnerabilidad de ejecución remota de código en los Servicios de Escritorio Remoto de Windows
CVE-2024-49108	8.1	Vulnerabilidad de ejecución remota de código en los Servicios de Escritorio Remoto de Windows
CVE-2024-49119	8.1	Vulnerabilidad de ejecución remota de código en los Servicios de Escritorio Remoto de Windows

Productos Afectados	
Microsoft Office	Microsoft Office Access
Microsoft Office Excel	Windows File Explorer
Windows Kernel	Microsoft Office Word
Windows Hyper-V	DNS Server
Windows 11	Windows 10
Windows server (Todas las versiones)	
Microsoft Office Publisher	
Microsoft Office SharePoint	
Windows Task Scheduler	
Windows Remote Desktop Services	
Windows LDAP - Lightweight Directory Access Protocol	
Windows Common Log File System Driver	

Categorías de las vulnerabilidades abordadas

- 27 vulnerabilidades de elevación de privilegios.
- 30 vulnerabilidades de ejecución remota de código.
- 7 vulnerabilidades de divulgación de información.
- 5 vulnerabilidades de denegación de servicio.
- 1 vulnerabilidad de suplantación de identidad.

Severidad: ALTA

Recomendaciones:

- Aplicar las actualizaciones de seguridad lo antes posible para proteger los sistemas de los riesgos potenciales.
- Priorizar la implementación de parches de seguridad, comenzando por las vulnerabilidades críticas y luego las calificadas como importantes.

Fuentes: Microsoft