e-dea NETWORKS | CYBER SECURITY

BOLETÍN INFORMATIVO

19 – Marzo - 2025

Vulnerabilidad en Microsoft Windows

Severidad: ALTA

Detalles:

Microsoft ha emitido un comunicado informando sobre vulnerabilidad identificada en sus productos.

Esta vulnerabilidad permite la exposición de información confidencial a un actor no autorizado en el Explorador de archivos de Windows facilitando la suplantación de identidad a través de una red.

Versiones afectadas:

Productos y versiones
Windows 10 versión 1809 para sistemas basados en x64
Windows 10 versión 1809 para sistemas de 32 bits
Windows Server 2025 (instalación de Server Core)
Servidor Windows 2025
Windows Server 2012 R2 (instalación de Server Core)
Servidor Windows 2012 R2
Windows Server 2016 (instalación de Server Core)
Servidor Windows 2016
Windows 10 versión 1607 para sistemas basados en x64
Windows 10 versión 1607 para sistemas de 32 bits
Windows 10 para sistemas basados en x64
Windows 10 para sistemas de 32 bits
Windows 11 versión 24H2 para sistemas basados en x64
Windows 11 versión 24H2 para sistemas basados en ARM64

Productos y versiones
Windows 11 versión 23H2 para sistemas basados en x64
Windows 11 versión 23H2 para sistemas basados en ARM64
Windows 10 versión 22H2 para sistemas de 32 bits
Windows 10 versión 22H2 para sistemas basados en ARM64
Windows 10 versión 22H2 para sistemas basados en x64
Windows 11 versión 22H2 para sistemas basados en x64
Windows 11 versión 22H2 para sistemas basados en ARM64
Windows 10 versión 21H2 para sistemas basados en x64
Windows 10 versión 21H2 para sistemas basados en ARM64
Windows 10 versión 21H2 para sistemas de 32 bits
Windows Server 2022 (instalación de Server Core)
Servidor Windows 2022
Windows Server 2019 (instalación de Server Core)
Servidor Windows 2019
Windows Server 2022, edición 23H2 (instalación de Server Core)

CVE Relacionada:

CVE	Tipo de vulnerabilidad
CVE-2025-24071	Windows File Explorer Spoofing Vulnerability

Severidad: ALTA

Recomendaciones:

- Microsoft ha lanzado oficialmente un parche de seguridad para corregir esta vulnerabilidad para las versiones de productos compatibles.
- Se recomienda que los usuarios afectados instalen el parche lo antes posible para su protección.