e-dea NETWORKS | CYBER SECURITY

BOLETÍN INFORMATIVO

18 - Septiembre -2024

Múltiples vulnerabilidades del fabricante microsoft

Detalles: +

El fabricante Microsoft emite comunicado sobre múltiples vulnerabilidades descubiertas de las cuales permiten ejecución de código, elevación de privilegios, omisión de funciones de seguridad, divulgación de información y denegación de servicios.

A continuación se detalla el número de errores en cada categoría de vulnerabilidad:

- 30 vulnerabilidades de elevación de privilegios.
- 4 vulnerabilidades de omisión de funciones de seguridad.
- 23 vulnerabilidades de ejecución remota de Código.
- 11 vulnerabilidades en la divulgación de información.
- 8 vulnerabilidades de denegación de servicio.
- 3 vulnerabilidades de suplantación de identidad.

Versiones afectadas:

- **Microsoft Office Word**
- **Microsoft Dynamics 365**
- **Microsoft Office Visio**
- **Microsoft Graphics Component**
- **SQL Server**
- **Azure Web Apps**
- **Windows DHCP Server**
- **Microsoft Office Publisher**
- **Microsoft Office Excel**
- **Microsoft Office SharePoint**
- **Windows Remote Desktop**
- **Microsoft Outlook for iOS**

CVE	CVSS	Tipo de vulnerabilidad
CVE-2024-38140	9.8	Vulnerabilidad de ejecución remota de código
CVE-2024-38109	9.1	Vulnerabilidad de elevación de privilegios
CVE-2024-38159	9.1	Vulnerabilidad de ejecución remota de código
CVE-2024-38160	9.1	Vulnerabilidad de ejecución remota de código
CVE-2024-38166	8.2	Vulnerabilidad de secuencias de comandos entre sitios (XSS)

Severidad: Crítica

CVE	CVSS	Tipo de vulnerabilidad
CVE-2024-38014	6.0	Vulnerabilidad de elevación de privilegios.
CVE-2024-38217	5.4	Vulnerabilidad de omisión de la función de seguridad.
CVE-2024-38226	7.3	Vulnerabilidad de omisión de la función de seguridad
CVE-2024-43491	7.1	Vulnerabilidad de ejecución remota de código

Severidad: Alta

Recomendaciones:

- Aplicar las actualizaciones de seguridad.
- Priorizar la implementación de parches de seguridad, comenzando por las vulnerabilidades críticas y luego las calificadas como importantes.
- Utilizar herramientas de gestión de parches para automatizar la distribución y aplicación de actualizaciones, garantizando así que todos los dispositivos dentro de la organización se mantengan actualizados de manera oportuna y consistente.

Fuentes: [Microsoft](), [Incibe](), [Mitre]()