e-dea NETWORKS | CYBER SECURITY

BOLETÍN
INFORMATIVO

16 - septiembre - 2026

Vulnerabilidad en CrowdStrike Falcon

El CVE-2026-40058 permite escritura en ubicaciones protegidas y posible elevación local de privilegios.

Afecta al sensor de Windows con "Microsoft Office File Malicious Macro Removal" habilitado.

Versiones afectadas y hotfixes

CVE-2026-40058 Falcon Sensor para Windows

Rama	Versión afectada	Corrección
8.10	8.10.21405	8.10.21408 y posteriores
7.40	7.40.21306	7.40.21309
7.39	7.39.21108 7.39.21105	7.39.21113
7.38 LTS	7.38.21003	7.38.21007 y siguientes actualizaciones 7.38 LTS
7.37	7.37.20907	7.37.20912
7.36	7.36.20805	7.36.20807

Versiones afectadas y hotfixes

CVE-2026-40058 Falcon Sensor para Windows

Rama	Versión afectada	Corrección
7.35	7.35.20709	7.35.20712
7.34	7.34.20610	7.34.20613
7.32 LTS	7.32.20406 (MR2) 7.32.20405 (MR1) 7.32.20403	7.32.20410 LTS
7.16*	7.16.18642 / 7.16.18637 7.16.18635 / 7.16.18632	7.16.18644

*Aplica para Windows 7 / Windows Server 2008 R2.

Otros productos y versiones

CVE-2026-40058 Falcon Sensor para Windows

Producto	Versión afectada	Corrección
Falcon Windows	7.33, 7.31 y anteriores	Migrar a una versión compatible con hotfix
Laroux Malware Cleanup Tool	1.3.65.0	1.4.70.0

** Sin soporte ni hotfix. Excepción: rama 7.16 para Windows 7 / 2008 R2.
Laroux utiliza la misma función vulnerable.

Recomendaciones



Severidad: **Alta**

CVSS 3.1: 8.8
CWE-367: condición de carrera

Parches

- *Instalar el hotfix correspondiente. Sustituir Laroux si se utiliza.*

Configuración

- *Después de actualizar, reactivar "Microsoft Office File Malicious Macro Removal" si se deshabilitó temporalmente.*

Fuente: CrowdStrike CVE-2026-40058