

26 DE OCTUBRE DE 2026

Boletín de ciberseguridad

Fortinet corrige fallos críticos en sus cortafuegos, HPE parchea su WiFi empresarial y Windows Server 2016 se acerca al fin de soporte. Revisa tus equipos de red y tus servidores.



FECHA	NOTICIAS	RIESGO MÁXIMO	WEB
26 de octubre de 2026	4	Alto	soporteinformatico360.com

■ Lo más importante de hoy

01. Fortinet corrige fallos críticos en FortiOS, FortiManager, FortiMail y otros

Riesgo Alto

INCIBE avisa de múltiples vulnerabilidades críticas y altas en varios productos de Fortinet, muy usados como cortafuegos en pymes. Fortinet publicará los detalles técnicos el 10 de noviembre, así que conviene actualizar antes.

A quién afecta: Empresas con cortafuegos FortiGate (FortiOS), FortiManager, FortiAnalyzer, FortiMail o FortiAuthenticator

Qué hacer

- ✓ Actualiza a FortiOS 8.0.2, 7.6.8, 7.4.13 o 7.2.14, o a la versión corregida de tu producto
- ✓ Limita la administración a IP de confianza y usa MFA
- ✓ No expongas FortiManager a Internet y guarda copia de la configuración

Fuente: INCIBE-CERT · <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-actualizaciones-en-productos-de-fortinet>

02. HPE corrige ocho fallos de gravedad máxima en su WiFi empresarial

Riesgo Alto

Aruba

HPE ha publicado parches para 72 vulnerabilidades en ArubaOS (AOS-8 y AOS-10), ocho de ellas de máxima gravedad. HPE no tiene constancia de que se estén explotando.

A quién afecta: Empresas con controladoras, puntos de acceso o pasarelas Aruba

Qué hacer

- ✓ Aplica las actualizaciones del aviso de HPE cuanto antes
- ✓ Activa el registro de actividad de los administradores
- ✓ Deja la gestión web y por consola solo en una red separada

Fuente: BleepingComputer · <https://www.bleepingcomputer.com/news/security/hpe-patches-eight-max-severity-rce-and-auth-bypass-aos-flaws/>

03. Un bootkit UEFI salta el arranque seguro de Windows en ataques dirigidos

Riesgo Medio

Kaspersky ha analizado BlackX, un malware que se carga antes que Windows aprovechando un fallo antiguo ya parcheado. Las víctimas tenían Windows al día, pero no habían aplicado las revocaciones adicionales de arranque seguro que Microsoft indica.

A quién afecta: Organizaciones con Windows; de momento, ataques de espionaje muy dirigidos

Qué hacer

- ✓ Mantén Windows y la BIOS actualizados
- ✓ Usa un antivirus actualizado y vigila alertas raras
- ✓ Revisa con tu técnico las instrucciones de Microsoft sobre revocaciones de arranque seguro

Fuente: BleepingComputer · <https://www.bleepingcomputer.com/news/security/blackx-uefi-bootkit-exploits-baton-drop-flaw-to-bypass-secure-boot/>

04. Windows Server 2016 dejará de recibir parches el 12 de enero de 2027

Riesgo Medio

Microsoft recuerda que la actualización de enero de 2027 será la última para todas las ediciones de Windows Server 2016. Después, los servidores quedarán sin protección ante nuevos fallos.

A quién afecta: Empresas y autónomos con servidores Windows Server 2016

Qué hacer

- ✓ Haz inventario de tus servidores y sus funciones
- ✓ Prueba antes con la versión de evaluación de 180 días
- ✓ Planifica la migración a Windows Server 2025 o a la nube

Fuente: BleepingComputer · <https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-server-2016-reaches-end-of-support-in-january/>



Consejo del día: Apunta en tu agenda la revisión mensual de cortafuegos, router y servidores: la mayoría de ataques aprovechan equipos de red sin actualizar.

¿Te preocupa alguna de estas amenazas?

Revisamos tus equipos y tu red sin compromiso.

Primer análisis técnico sin coste para empresas.

910 117 112

soporte@soporteinformatico360.com

soporteinformatico360.com