

20 DE OCTUBRE DE 2026

Boletín de ciberseguridad

Hoy destacan dos ataques a la cadena de suministro (AOMEI Backupper y el plugin Rank Math PRO), un fallo crítico explotado en BeyondTrust y problemas de Exchange tras los parches de octubre.



FECHA
20 de octubre de 2026

NOTICIAS
4

RIESGO MÁXIMO
Alto

WEB
soporteinformatico360.com

■ Lo más importante de hoy

01. Atacantes usaron los servidores de AOMEI para colar malware

Riesgo Alto

Según Mandiant y ManageEngine, entre abril y julio de 2026 unos atacantes alteraron durante minutos la configuración de actualizaciones de AOMEI Backupper para instalar puertas traseras (CROSSROAD y SHINYROAD) en algunos equipos. AOMEI ya ha reforzado sus servidores, pero eso no limpia los equipos que se infectaron entonces.

A quién afecta: Particulares y empresas que usan AOMEI Backupper en Windows

Qué hacer

- ✓ Actualiza AOMEI Backupper a la última versión
- ✓ Busca tareas programadas raras y Radmin instalado sin motivo
- ✓ Pasa un análisis completo con tu antivirus
- ✓ Si tienes dudas, pide una revisión del equipo

Fuente: BleepingComputer · <https://www.bleepingcomputer.com/news/security/hackers-hijack-aomei-update-servers-to-secretly-spread-malware/>

02. El plugin Rank Math PRO de WordPress se distribuyó con una puerta trasera

Riesgo Alto

La versión 3.0.123 de Rank Math PRO descargada de la web oficial entre el 15 y el 16 de octubre traía código malicioso que da acceso permanente a la web y expone contraseñas y claves. La versión gratuita de WordPress.org no está afectada y la 3.0.124 ya está limpia.

A quién afecta: Negocios y autónomos con web WordPress que usan Rank Math PRO

Qué hacer

- ✓ Comprueba qué versión de Rank Math PRO tienes
- ✓ Si activaste la 3.0.123, restaura una copia limpia
- ✓ Busca administradores nuevos con usuario wpsupport_
- ✓ Cambia contraseñas, claves API y salts

Fuente: BleepingComputer · <https://www.bleepingcomputer.com/news/security/wordpress-seo-plugin-rank-math-compromised-to-back-door-websites/>

03. Fallo crítico explotado en BeyondTrust Remote Support

Riesgo Alto

INCIBE-CERT avisa de la vulnerabilidad CVE-2026-102764 en BeyondTrust Remote Support hasta la versión 26.2.3. Permite a un atacante remoto sin credenciales manipular archivos del equipo y ya se ha explotado. Los clientes en la nube ya están parcheados desde el 9 de octubre.

A quién afecta: Empresas con BeyondTrust Remote Support instalado en sus servidores

Qué hacer

- ✓ Aplica el parche BT26-05-RS
- ✓ Si tienes una versión anterior a 24.3.1, actualiza primero
- ✓ Revisa los registros de acceso remoto

Fuente: INCIBE-CERT · <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/validacion-incorrecta-del-origen-en-remote-support-de-beyondtrust>

04. Las actualizaciones de octubre de Windows Server afectan a Exchange

Riesgo Medio

Microsoft confirma que los parches de octubre para Windows Server 2019 y posteriores pueden impedir entrar en Outlook o en OWA y dejar correos atascados en la Bandeja de salida en servidores Exchange con mucha carga. Microsoft pide no desinstalar las actualizaciones.

A quién afecta: Pymes con servidor Exchange propio

Qué hacer

- ✓ No desinstales las actualizaciones
- ✓ Aplica la solución temporal publicada por Microsoft
- ✓ Vigila el envío de correo tras reiniciar

Fuente: BleepingComputer · <https://www.bleepingcomputer.com/news/microsoft/microsoft-october-windows-server-updates-cause-exchange-issues/>



Consejo del día: Que un programa se actualice solo no garantiza que esté limpio: ten copias de seguridad desconectadas y revisa de vez en cuando qué tareas programadas y programas de acceso remoto tienes instalados.

¿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