

21 DE OCTUBRE DE 2026

Boletín de ciberseguridad

Hoy destacan un programa de copias de seguridad cuyas actualizaciones fueron manipuladas, un plugin de WordPress comprometido y fallos graves en herramientas de soporte remoto.



FECHA	NOTICIAS	RIESGO MÁXIMO	WEB
21 de octubre de 2026	5	Alto	soporteinformatico360.com

■ Lo más importante de hoy

01. Manipulan las actualizaciones de AOMEI Backupper para colar malware

Riesgo Alto

Atacantes alteraron durante unos minutos, en varias fechas entre mayo y julio de 2026, los servidores de actualización de AOMEI Backupper para descargar un troyano. AOMEI dice que ya lo ha corregido, pero eso no limpia los equipos que ya se infectaron.

A quién afecta: Usuarios y empresas con AOMEI Backupper en Windows

Qué hacer

- ✓ Revisa con tu antivirus los equipos que tienen AOMEI
- ✓ Busca tareas programadas o programas extraños en su carpeta
- ✓ Si sospechas infección, pide ayuda a un técnico

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

02. Plugin Rank Math PRO para WordPress comprometido

Riesgo Alto

La versión 3.0.123 de Rank Math PRO descargada de la web oficial entre el 15 y el 16 de octubre llevaba una puerta trasera. La versión gratuita no está afectada y ya existe la 3.0.124 limpia.

A quién afecta: Negocios con web en WordPress que usen Rank Math PRO

Qué hacer

- ✓ Comprueba si instalaste la 3.0.123 esos días
- ✓ Restaura una copia limpia y cambia todas las claves
- ✓ Instala la versión 3.0.124

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

03. Fallo crítico en BeyondTrust Remote Support, ya explotado

Riesgo Alto

Una vulnerabilidad crítica (CVE-2026-102764) en Remote Support hasta la versión 26.2.3 permite a un atacante sin credenciales operar con archivos del equipo. Se explotó en agosto. En la nube ya está corregido.

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

Qué hacer

- ✓ Aplica el parche BT26-05-RS
- ✓ Actualiza versiones anteriores a la 24.3.1
- ✓ Revisa los registros de acceso

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

04. Vulnerabilidad alta en MobaXterm Portable

Riesgo Medio

MobaXterm Personal Edition Portable 26.4 no comprueba la integridad de uno de sus componentes, lo que permitiría ejecutar código malicioso si alguien puede modificar sus archivos. No consta que se haya explotado.

A quién afecta: Técnicos y empresas que usan MobaXterm en Windows

Qué hacer

- ✓ Actualiza a la versión 26.5 o posterior
- ✓ Descarga solo desde la web oficial

Fuente: INCIBE-CERT · <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/ausencia-de-verificacion-de-integridad-en-mobaxterm-de-mobatek>

05. Microsoft corrige los cierres de juegos y apps en Windows 11

Riesgo Bajo

La actualización opcional KB5124010 de septiembre hacía que algunos juegos y apps con audio Dolby Digital se cerraran. La actualización de seguridad de octubre, KB5127648, lo soluciona.

A quién afecta: Usuarios de Windows 11 24H2 o posterior

Qué hacer

- ✓ Instala las actualizaciones de octubre desde Windows Update
- ✓ Reinicia el equipo tras actualizar

Fuente: BleepingComputer · <https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-game-app-crashes-caused-by-windows-kb5124010-preview-update/>



Consejo del día: Ni las actualizaciones oficiales son infalibles: mantén copias de seguridad desconectadas y un antivirus activo para detectar a tiempo cualquier cosa extraña.

¿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