

16 DE OCTUBRE DE 2026

Boletín de ciberseguridad

INCIBE avisa de cuentas de WhatsApp en iPhone sin actualizar que se usan para pedir dinero a sus contactos. Además, varios fabricantes de cortafuegos, VPN y correo para empresas corrigen fallos graves que ya se están aprovechando.



FECHA

16 de octubre de 2026

NOTICIAS

5

RIESGO MÁXIMO

Alto

WEB

soporteinformatico360.com

Lo más importante de hoy

01. Usan WhatsApp de iPhones sin actualizar para pedir dinero

Riesgo Alto

Los contactos de la víctima reciben mensajes que ella no ha escrito, pidiendo unos cientos de euros por una supuesta urgencia. La víctima sigue usando WhatsApp con normalidad y no ve esos mensajes. La mayoría de casos atendidos por INCIBE eran iPhone con versiones antiguas de iOS.

A quién afecta: Personas con WhatsApp en iPhone sin actualizar y todos sus contactos

Qué hacer

- ✓ Actualiza iOS y WhatsApp
- ✓ Activa la verificación en dos pasos
- ✓ Revisa los dispositivos vinculados
- ✓ Antes de pagar, llama a la persona

Fuente: INCIBE Ciudadanía · <https://www.incibe.es/ciudadania/avisos/los-ciberdelincuentes-estan-utilizando-cuentas-de-whatsapp-en-iphone-sin>

02. Fallo explotado en la VPN Ivanti Connect Secure

Riesgo Alto

Ivanti ha corregido una vulnerabilidad que permite a un atacante, sin usuario ni contraseña, saltarse el acceso y ejecutar órdenes en el equipo VPN. El fabricante confirma que ya se ha usado en ataques, aunque de forma limitada.

A quién afecta: Empresas que usan Ivanti Connect Secure para el teletrabajo

Qué hacer

- ✓ Actualiza a la versión corregida
- ✓ Pasa la herramienta de integridad
- ✓ Guarda registros si sospechas algo

Fuente: INCIBE-CERT · <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-ivanti-4>

03. Cisco corrige fallos críticos en su pasarela de correo

Riesgo Alto

Cisco ha publicado seis vulnerabilidades en Secure Email Gateway y Secure Email and Web Manager, cinco de ellas críticas. Una, ya explotada, permite tomar el control del equipo con solo enviarle un adjunto preparado.

A quién afecta: Empresas que filtran su correo con equipos Cisco Secure Email

Qué hacer

- ✓ Actualiza a la versión corregida
- ✓ Si sospechas, cambia credenciales
- ✓ Revisa que las actualizaciones automáticas estén activas

Fuente: INCIBE-CERT · <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-productos-de-cisco-17>

04. Vulnerabilidad en los cortafuegos de Palo Alto Networks

Riesgo Medio

Un fallo en el panel de administración de PAN-OS permite a un atacante con acceso de administrador ejecutar código con control total del cortafuegos. El fabricante ha visto una explotación muy limitada.

A quién afecta: Empresas con cortafuegos Palo Alto (PA-Series, VM-Series y Panorama)

Qué hacer

- ✓ Actualiza PAN-OS a la versión corregida
- ✓ No dejes el panel accesible desde Internet
- ✓ Revisa quién tiene acceso de administrador

Fuente: INCIBE-CERT · <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/inyeccion-de-codigo-en-pan-os-de-palo-alto-networks>

05. Fallos en TSplus Remote Access, usado para el acceso remoto

Riesgo Medio

INCIBE ha coordinado la publicación de tres vulnerabilidades, descubiertas por un investigador español. Una permite entrar sin el segundo factor de autenticación si el atacante conoce la contraseña. No se conoce explotación.

A quién afecta: Pymes que usan TSplus para acceder a sus programas a distancia

Qué hacer

- ✓ Instala la última versión de TSplus
- ✓ Usa contraseñas largas y únicas
- ✓ Revisa los accesos recientes

Fuente: INCIBE-CERT · <https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-tsplus-remote-access>



Consejo del día: Si alguien te pide dinero por WhatsApp, aunque sea un familiar, llámale antes de hacer nada. Y en la empresa, los equipos que dan acceso desde fuera (VPN, cortafuegos, escritorio remoto) son los primeros que hay que 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