Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

LA OFENSIVA RUSA CONTRA LA INFRAESTRUCTURA DIGITAL GLOBAL

21/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

Recientemente, el FBI advierte que el grupo estatal ruso FSB Centro 16 está explotando una antigua vulnerabilidad (CVE-2018-0171) en dispositivos de red Cisco que ejecutan Smart Install (SMI). Esta explotación se enfoca en la infraestructura crítica tanto en EE. UU. como a nivel global.

LA OFENSIVA RUSA CONTRA LA INFRAESTRUCTURA DIGITAL GLOBAL

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_08_21_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	21/08/2025
Es día cero (0 day):	No

RESUMEN

Recientemente, el FBI advierte que el grupo estatal ruso FSB Centro 16 está explotando una antigua vulnerabilidad (CVE-2018-0171) en dispositivos de red Cisco que ejecutan Smart Install (SMI). Esta explotación se enfoca en la infraestructura crítica tanto en EE. UU. como a nivel global.

¿Cómo se lleva a cabo?

En lo que va del último año, los investigadores encontraron que los cibercriminales recopilaron archivos de configuración de miles de equipos de infraestructura crítica. En dichos equipos, modificaron las configuraciones para mantener acceso no autorizado a los dispositivos.

¿Qué es Cisco Smart Install (SMI)?

Esta función facilita la configuración automática de switches Cisco en redes grandes, lo que permite que un switch recién instalado descargue su configuración desde un servidor maestro sin intervención manual.

El problema radica en que SMI nunca fue diseñado con seguridad. Utiliza un protocolo sin autenticación ni cifrado, lo cual lo hace potencialmente vulnerable.

¿En qué consiste la vulnerabilidad explotada?

La vulnerabilidad consiste en un desbordamiento de memoria. Un cibercriminal puede enviar paquetes malformados al puerto TCP/4786, que es el puerto usado para SMI. Esto le permite al atacante ejecutar código arbitrario en el dispositivo o causar una denegación de servicio (DoS), reiniciando el equipo.

Si lo vemos de una forma más sencilla, es como si cualquiera pudiera mandar órdenes a tu switch sin contraseña y, en algunos casos, tomar el control completo.

¿Por qué sigue siendo crítico en 2025 si la vulnerabilidad es de 2018?

Muchos dispositivos de Cisco siguen siendo utilizados sin actualizarse, sobre todo en infraestructuras críticas. Además, en algunas organizaciones, ni siquiera saben que SMI está habilitado en sus equipos. Esto abre una oportunidad para los cibercriminales.

RECOMENDACIONES

- Instala las últimas versiones de firmware que corrigen la vulnerabilidad.
- Verifica siempre en el portal oficial de Cisco Security Advisories si tu modelo está afectado.
- Muchos entornos tienen SMI activo sin necesidad. Si no lo necesitas, desactívalo completamente para cerrar el vector de ataque.
- Aplica reglas en firewalls o ACLs para permitir solo la comunicación de dispositivos autorizados.

NOTICIA COMPLETA

https://devel.group/blog/la-ofensiva-rusa-contra-la-infraestructura-digital-global/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group