Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

LOCKBIT SUFRE FILTRACIÓN SE EXPONEN MENSAJES DE NEGOCIACIÓN Y CONTRASEÑAS DE AFILIADOS

09 / 05 / 2025

CONTENIDO

INTRODUCCIÓN

En un nuevo golpe contra el cibercrimen, el temido grupo de ransomware LockBit ha sido hackeado y expuesto públicamente. Su panel de afiliados en la dark web fue intervenido y reemplazado por un mensaje burlón que incluía un enlace con su base de datos interna. Entre los datos filtrados se encuentran miles de direcciones de Bitcoin, configuraciones de ataques, mensajes de negociación con víctimas y hasta contraseñas de sus miembros. Esta filtración pone en jaque la reputación del grupo y demuestra que, incluso en el mundo del crimen digital, nadie está a salvo.

LOCKBIT SUFRE FILTRACIÓN: SE EXPONEN MENSAJES DE NEGOCIACIÓN Y CONTRASEÑAS DE AFILIADOS

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

ID de alerta:	DSOC-CERT_2025_05_09_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	09/05/2025
Es día cero (0 day):	No

RESUMEN

¿Qué la hace tan peligrosa?
El fallo se debe a la presencia de un token JWT (JSON Web Token) codificado de forma fija en los dispositivos afectados. Un atacante podría aprovecharlo enviando solicitudes HTTPS manipuladas para:

- Subir archivos arbitrarios
- Navegar por los directorios del sistema
- Ejecutar comandos con control total (*root*)

¿Qué equipos están en riesgo?
Solo si tiene activada la función "Out-of-Band AP Image Download" (desactivada por defecto), los siguientes dispositivos pueden ser vulnerables:

- Catalyst 9800-CL Wireless Controllers for Cloud
- Catalyst 9800 Embedded Wireless Controller para switches Catalyst 9300, 9400 y 9500
- Catalyst 9800 Series Wireless Controllers
- Embedded Wireless Controller en puntos de acceso Catalyst (APs)

¿Qué se debe hacer?

- Actualiza inmediatamente a las versiones corregidas que Cisco ha publicado.
- Como medida temporal, si no puedes actualizar aún, desactiva la función "Out-of-Band AP Image Download" para mitigar el riesgo. Esto no afecta el funcionamiento de los APs, que seguirán actualizándose vía CAPWAP.

Puedes consultar las versiones corregidas y los detalles técnicos en el sitio oficial de Cisco: https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu

¿Se ha usado esta vulnerabilidad en ataques reales?
No, según Cisco, no hay evidencia de explotación activa en el mundo real. La falla fue descubierta internamente por su equipo de seguridad ASIG.

NOTICIA COMPLETA

https://devel.group/blog/cisco-corrige-una-vulnerabilidad-critica-en-controladores-ios-xe-cve-2025-20188/

CONTACTOS DE SOPORTE

Correo electrónico: soporte@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/