



PERÚ

Presidencia
del Consejo de Ministros

Secretaría de Gobierno
y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL



 Asociación de
Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

239-2025-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.


La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Vulnerabilidades críticas en teléfonos Cisco permiten ataques de denegación de servicio y ejecución de código malicioso 4

Vulnerabilidades en productos Cisco. 6

Índice alfabético 7

 Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°239		Fecha: 17-10-2025
			Página: 4 de 7
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Vulnerabilidades críticas en teléfonos Cisco permiten ataques de denegación de servicio y ejecución de código malicioso		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	Malware
Medios de propagación	Red , Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

El Centro Nacional de Seguridad Digital informa sobre vulnerabilidades detectadas en los teléfonos Cisco Desk, IP y Video, que podrían ser explotadas para ejecutar ataques de denegación de servicio (DoS) y cross-site scripting (XSS) de forma remota.

Los modelos afectados incluyen las series Desk Phone 9800, IP Phone 7800 y 8800, y Video Phone 8875, cuando se encuentran registrados en Cisco Unified Communications Manager con la opción Web Access habilitada. No existen soluciones temporales, por lo que la actualización inmediata a las versiones corregidas es esencial.



Ilustración 1: Vulnerabilidades críticas en teléfonos Cisco (Fuente: GBHackers.com)

2. DETALLES:

Cisco publicó el **boletín cisco-sa-phone-dos-FPyjLV7A** el 15 de octubre de 2025, donde detalla dos vulnerabilidades críticas:

- **CVE-2025-20350 (7.5 – Alta):** Permite a un atacante no autenticado enviar paquetes HTTP maliciosos que provocan un **desbordamiento de búfer**, reiniciando el dispositivo y causando una condición de **DoS**.
- **CVE-2025-20351 (6.1 – Media):** Posibilita la **inyección de scripts** a través de entradas no validadas, generando ataques **XSS** en la interfaz web del dispositivo.

Ambas vulnerabilidades requieren que **Web Access esté activado** (función deshabilitada por defecto).

Los modelos corregidos incluyen:

- **Desk Phone 9800 Series:** SIP Software 3.3(1) o superior.
- **IP Phone 7800/8800 Series:** versión 14.3(1)SR2 o superior.
- **Video Phone 8875:** SIP Software 3.3(1) o superior.

3. RECOMENDACIONES:


El Centro Nacional de Seguridad Digital recomienda a las organizaciones que:

- Actualicen de inmediato todos los dispositivos a las versiones mencionadas.
- Verifiquen el estado del Web Access y lo deshabiliten temporalmente si no es indispensable.
- Planifiquen las actualizaciones en una ventana de mantenimiento para evitar interrupciones.
- Utilicen la herramienta Bulk Administration Tool para aplicar los cambios de forma masiva.
- Mantengan monitoreo constante de los avisos de seguridad de Cisco y apliquen parches sin demora.

La pronta implementación de estas medidas permitirá preservar la disponibilidad y seguridad de la infraestructura de comunicaciones institucional frente a amenazas activas.

Fuente de Información:

- <https://gbhackers.com/cisco-desk-ip-and-video-phones-vulnerable/>

	ALERTA DE SEGURIDAD DIGITAL N°709		Fecha: 17-10-2025
			Página: 6 de 7
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades en productos Cisco.		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		
Descripción			
<p>1. ANTECEDENTES:</p> <p>Cisco Systems, Inc. ha publicado dos vulnerabilidades de severidad CRÍTICA clasificadas como CWE-127: Buffer subleído y CWE-805: Acceso al búfer con un valor de longitud incorrecto en el decodificador MIME (Extensiones de correo de Internet multipropósito) HTTP que afectan a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado provocar que el motor de detección Snort 3 filtre posible información confidencial o se reinicie.</p> <p>2. DETALLES:</p> <p>La vulnerabilidad de severidad media identificada por MITRE como CVE-2025-20359 de divulgación de información MIME o denegación de servicio en Snort 3 que afecta a varios productos de Cisco. La vulnerabilidad en el decodificador HTTP Snort 3 podría permitir que un atacante remoto no autenticado provoque la divulgación de posibles datos confidenciales o provoque el bloqueo del motor de detección Snort 3. Esta vulnerabilidad se debe a un error en la lógica de gestión del búfer al analizar los campos MIME del encabezado HTTP. Esto puede provocar una lectura insuficiente del búfer. Un atacante podría explotar esta vulnerabilidad enviando paquetes HTTP manipulados a través de una conexión establecida analizada por Snort 3. Una explotación exitosa podría permitir al atacante inducir uno de dos posibles resultados: el reinicio inesperado del motor de detección de Snort 3, lo que podría causar una denegación de servicio (DoS), o la divulgación de información confidencial en el flujo de datos de Snort 3. Debido a la lectura insuficiente, es posible que se devuelva información confidencial que no sea datos de conexión válidos.</p> <p>La vulnerabilidad de severidad media identificada por MITRE como CVE-2025-20360 en el decodificador HTTP Snort 3 que podría permitir que un atacante remoto no autenticado provoque el reinicio del motor de detección Snort 3. Esta vulnerabilidad se debe a la falta de una comprobación completa de errores al analizar los campos MIME del encabezado HTTP. Un atacante podría explotar esta vulnerabilidad enviando paquetes HTTP manipulados a través de una conexión establecida para que Snort 3 los analice. Una explotación exitosa podría permitir al atacante provocar una denegación de servicio (DoS) cuando el motor de detección de Snort 3 se reinicie inesperadamente.</p> <p>A. Productos afectados:</p> <ul style="list-style-type: none"> ➤ Software Cisco Secure Firewall Threat Defense (FTD) si está configurado con Snort 3, versión 3.x. ➤ Cisco Cyber Vision, versiones anteriores a 5.3. ➤ Asimismo, estas vulnerabilidades también afectan a los siguientes productos de Cisco si ejecutaban una versión vulnerable de Unified Threat Defense (UTD) Snort IPS Engine para Cisco IOS XE Software o UTD Engine para Cisco IOS XE SD-WAN Software: <ul style="list-style-type: none"> ▪ Enrutadores de servicios integrados (ISR) de la serie 1000. ▪ ISR de la serie 4000. ▪ Software de borde Catalyst 8000V. ▪ Plataformas perimetrales de la serie Catalyst 8200. ▪ Plataformas perimetrales de la serie Catalyst 8300. ▪ Plataformas de borde Catalyst 8500L. ▪ Enrutadores de servicios en la nube de 1000 V. ▪ Enrutadores virtuales de servicios integrados. <p>3. RECOMENDACIONES:</p> <p>Cisco ha publicado actualizaciones de software que solucionan estas vulnerabilidades. No existen soluciones alternativas que las solucionen.</p>			
Fuente de Información:	<ul style="list-style-type: none"> • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-snort3-mime-vulns-tTL8PgVH 		

Índice alfabético

Malware 4

Explotación de vulnerabilidades conocidas 6