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

131-2025-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 Aéreadel 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 lasempresas 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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°131	Fecha: 06-06-2025
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Botnet BADBOX 2.0 infecta millones de dispositivos en América Latina		
Tipo de Ataque	Botnets	Abreviatura	Botnets
Medios de propagación	IRC, USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

El FBI advierte que la campaña de malware BADBOX 2.0 ha infectado más de un millón de dispositivos domésticos conectados a Internet.

2. DETALLES:

Esta botnet afecta a productos electrónicos de consumo como televisores inteligentes, proyectores, tablets y dispositivos IoT de bajo costo, la mayoría fabricados en China y con sistema Android.

Lo más inquietante es que muchos de estos equipos vienen infectados de fábrica o se contaminan después, al instalar apps maliciosas o actualizaciones de firmware. Una vez infectados, estos dispositivos se convierten en nodos de una red de proxies residenciales, usados por ciberdelincuentes para ocultar su identidad y llevar a cabo actividades ilegales.

Una vez que estos dispositivos IoT comprometidos se conectan a las redes domésticas, son susceptibles de formar parte de la botnet BADBOX 2.0. Una vez infectados, los dispositivos se conectan a los servidores de comando y control (C2) del atacante, donde reciben comandos para ejecutar en los dispositivos comprometidos, como:

- **Redes proxy residenciales:** El malware dirige el tráfico de otros ciberdelincuentes a través de las direcciones IP de las víctimas, enmascarando la actividad maliciosa.
- **Fraude publicitario:** BADBOX puede cargar y hacer clic en anuncios en segundo plano, generando ingresos publicitarios para los actores de la amenaza.
- **Relleno de credenciales:** Al aprovechar las IP de las víctimas, los atacantes intentan acceder a las cuentas de otras personas utilizando credenciales robadas.

Hay varias señales que pueden ayudarte a darte cuenta si algo anda mal:

- Te aparecen aplicaciones raras que nunca descargaste.
- El equipo viene con Google Play Protect desactivado o directamente no está certificado.
- Lo promocionaron como “desbloqueado” o como si te diera acceso gratis a servicios de paga.
- Tu red de internet se comporta extraño, como si siempre estuviera mandando o recibiendo datos.
- La marca del dispositivo suena genérica o no la conoces para nada.

3. RECOMENDACIONES:

- Revisar todos los aparatos conectados a tu red WiFi, para identificar alguno sospechoso o no reconcido.
- No instalar apps desde tiendas no oficiales. Si una aplicación promete contenido gratuito que normalmente es de paga, probablemente algo anda mal.
- Monitorear el tráfico de internet, hacia y desde las redes domésticas. Hay routers o apps que te pueden ayudar a ver si un dispositivo está enviando datos sin motivo.
- Mantener todos tus equipos actualizados. Las actualizaciones corrigen errores de seguridad.
- Desconectar de internet cualquier equipo que parece estar infectado. Interrumpir el funcionamiento del malware y evitar que se comunique con los atacantes.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2025/06/botnet-badbox-20-infecta-millones-de.html • hxxps://blog.tecnetone.com/malware-badbox-2.0-viene-instalado-en-millones-de-dispositivos-android

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°131	Fecha: 06-06-2025 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el software del controlador inalámbrico Cisco IOS XE		
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

1. ANTECEDENTES:

Cisco Systems, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo uso de credenciales codificadas en las funciones de descarga de imágenes de puntos de acceso (AP) fuera de banda, grabación espectral de aire limpio y paquetes de depuración de clientes del software Cisco IOS XE para controladores de LAN inalámbrica (WLC). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado cargue archivos arbitrarios en un sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-20188 de tipo uso de credenciales codificadas en las funciones de descarga de imágenes de AP fuera de banda, grabación espectral de aire limpio y paquetes de depuración de clientes del software Cisco IOS XE para WLC, podría permitir a un atacante remoto no autenticado cargue archivos arbitrarios en un sistema afectado.

Esta vulnerabilidad se debe a la presencia de un token web JSON (JWT) codificado de forma rígida en un sistema afectado. Un atacante podría explotar esta vulnerabilidad enviando solicitudes HTTPS manipuladas a la interfaz de carga de archivos del punto de acceso. Una explotación exitosa podría permitir al atacante cargar archivos, atravesar rutas y ejecutar comandos arbitrarios con privilegios de root.

A. Productos afectados:

Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco IOS XE para WLC, independientemente de la configuración del dispositivo:

- Controladores inalámbricos Catalyst 9800-CL para la nube.
- Controlador inalámbrico integrado Catalyst 9800 para conmutadores de las series Catalyst 9300, 9400 y 9500.
- Controladores inalámbricos de la serie Catalyst 9800.
- Controlador inalámbrico integrado en puntos de acceso Catalyst.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°131	Fecha: 06-06-2025
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Google ChromeOS LTS		
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

1. ANTECEDENTES:

Se ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo lectura y escritura fuera de límites que afecta a Google ChromeOS LTS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema objetivo.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-5419 de tipo escritura fuera de límites que afecta a Google ChromeOS LTS, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema objetivo.

La vulnerabilidad existe debido a un error de límite en el motor V8. Un atacante remoto puede engañar a la víctima para que visite un sitio web especialmente diseñado, activar una escritura fuera de límites y ejecutar código arbitrario en el sistema objetivo. Esta vulnerabilidad se está explotando activamente en la naturaleza por múltiples actores de amenaza.

A. Productos afectados:

- Chrome OS: versiones anteriores a 137.0.7151.68.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://chromereleases.googleblog.com/2025/06/long-term-support-channel-update-for.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°131	Fecha: 06-06-2025 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Microsoft Power Automate		
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

1. ANTECEDENTES:

Microsoft Corporation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo exposición de información sensible a un actor no autorizado en Microsoft Power Automate para escritorio. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado elevar privilegios en una red.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-47966 de tipo exposición de información sensible a un actor no autorizado en Microsoft Power Automate, podría permitir a un atacante remoto no autenticado basados en la red exponer información confidencial y elevar privilegios en una red sin interacción del usuario ni privilegios previos.

La vulnerabilidad existe debido a un control de acceso o validación inadecuados en los mecanismos de transferencia de datos de Power Automate, lo que permite a los atacantes con acceso a la red interceptar o manipular solicitudes que revelan información privilegiada, como tokens de autenticación, metadatos de flujo de trabajo o credenciales integradas.

A. Productos afectados:

- Microsoft Power Automate.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Aplicar parches inmediatamente en todos los entornos de Power Automate.
- Auditar permisos, habilitar la autenticación multifactor, monitorear las actividades anómalas y aplicar principios de privilegio mínimo a conectores y flujos de trabajo.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47966

Índice alfabético