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

142-2025-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°142	Fecha: 19-06-2025 Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Alerta por filtración de contraseñas que expone a 16.000 millones de cuentas de todo el mundo		
Tipo de Ataque	Fuga de Información	Abreviatura	FugaInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K02
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

Varias recopilaciones de credenciales de inicio de sesión revelan una de las mayores filtraciones de datos de la historia, con un total de 16 000 millones de credenciales expuestas. Es muy probable que los datos provengan de diversos ladrones de información.

2. DETALLES:

Esta gran cantidad de conjuntos de datos, descubierta y catalogada por el equipo de Cybernews, que hasta ahora habían pasado mayormente desapercibidas para la vista pública, no se habían reportado hasta la fecha. Así, dicha brecha se ha posicionado como una de las más importantes de la historia reciente.

No se sabe con certeza quién es el propietario de los datos filtrados. Si bien podrían ser investigadores de seguridad quienes recopilan datos para verificar y monitorear las filtraciones, es prácticamente seguro que algunos de los conjuntos de datos filtrados pertenecían a ciberdelincuentes.

Es imposible determinar cuántas personas o más bien cuántas cuentas han sido afectadas por esta brecha de datos, pues no equivalen a 16.000 millones de personas hackeadas o afectadas, sino a una mezcla de contraseñas, información de robo de datos, información sobre malware usado para estos robos, etc.

La mayoría de datos seguían el siguiente esquema: URL, datos de inicio de sesión (por ejemplo, nombres de usuario) y una contraseña asociada.

Los expertos advierten que la inclusión de registros de infostealer tanto antiguos como recientes, a menudo con tokens, cookies y metadatos, hace que estos datos sean particularmente peligrosos para las organizaciones que carecen de autenticación multifactor o prácticas de higiene de credenciales.

Entre los datos expuestos, se incluyen tres lotes distintos que superan los mil millones de credenciales cada uno. El lote más grande, con 3500 millones de credenciales, se originó en poblaciones de habla portuguesa. Otros lotes importantes se asociaron con inicios de sesión rusos y de Telegram. Los datos en los conjuntos filtrados son una mezcla de detalles de malware que roba información (infostealer malware), conjuntos de credential stuffing y filtraciones reempaquetadas.

La información de los conjuntos de datos filtrados abre las puertas a prácticamente cualquier servicio en línea imaginable, desde Apple, Facebook y Google hasta GitHub, Telegram y diversos servicios gubernamentales.

Los ciberdelincuentes ahora tienen un acceso sin precedentes a credenciales personales que pueden ser utilizadas para la toma de control de cuentas, el robo de identidad, intrusiones de ransomware, campañas de phishing altamente dirigido, y ataques de compromiso de correo electrónico empresarial (BEC).

3. RECOMENDACIONES:

- Se insta a la población que renueve sus contraseñas de todas las plataformas, aplicativos y redes sociales.
- Aplicar políticas de contraseñas seguras. Cambiar las contraseñas de todas sus cuentas de manera periódica utilizando una contraseña fuerte y única para cada sitio.
- Activar el doble factor de autenticación en todo donde sea posible.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Utilizar gestores de contraseñas, considerando aquellos casos en los que tengamos que recordar un gran número de ellas para acceder a muchos servicios. En estos casos es muy recomendable elegir un gestor cuyo control quede bajo nuestra supervisión, que cifre las credenciales e implante doble factor de autenticación para acceder al mismo. Y la más importante característica sería el Generador de contraseñas, el cual permite crear contraseñas aleatorias seguras para los diferentes servicios automáticamente.
- Revocar de inmediato los accesos de personal que cese en sus funciones o cambie de puesto.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de los ataques.
- Publicar la recomendación de no utilizar la misma contraseña para servicios diferentes, o establecer una política al respecto.
- No compartir credenciales de acceso bajo ninguna circunstancia. El acceso es personal e intransferible.
- Capacitar a los usuarios sobre las políticas de seguridad y privacidad de la información, así como sobre el uso ético y legal de los datos a los que acceden.

Fuente de Información:	• hxxps://www.elespanol.com/omicrono/software/20250619/peligro-millones-contrasenas-mayores-filtraciones-historia/1003743812648_0.html • hxxps://www.lanacion.com.ar/tecnologia/una-filtracion-masiva-expone-a-16000-millones-de-cuentas-en-todo-el-mundo-nid19062025/ • hxxps://www.ambito.com/tecnologia/alerta-filtracion-contrasenas-que-expone-16000-millones-cuentas-todo-el-mundo-n6158407 • hxxps://cybernews.com/security/billions-credentials-exposed-infostealers-data-leak/ • hxxps://appleinsider.com/articles/25/06/18/16-billion-logins-discovered-across-exposed-datasets-but-dont-panic

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°142	Fecha: 19-06-2025 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad 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

1. ANTECEDENTES:

Cisco Systems, Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo uso de variables no inicializadas que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado provocar una condición de denegación de servicio (DoS) en el servicio Cisco AnyConnect de un dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-20271 de tipo uso de variables no inicializadas en el servidor VPN de Cisco AnyConnect de los dispositivos Cisco Meraki MX y Cisco Meraki Z Series Teleworker Gateway, podría permitir que un atacante remoto no autenticado provoque una condición de denegación de servicio (DoS) en el servicio Cisco AnyConnect en un dispositivo afectado.

Esta vulnerabilidad se debe a errores de inicialización variables al establecer una sesión VPN SSL. Un atacante podría explotar esta vulnerabilidad enviando una secuencia de solicitudes HTTPS manipuladas a un dispositivo afectado. Si se logra explotar, el atacante podría reiniciar el servidor VPN de Cisco AnyConnect, lo que provocaría el fallo de todas las sesiones VPN SSL establecidas y obligaría a los usuarios remotos a iniciar una nueva conexión VPN y a autenticarse de nuevo. Un ataque continuo podría impedir el establecimiento de nuevas conexiones VPN SSL, lo que haría que el servicio VPN de Cisco AnyConnect no estuviera disponible para todos los usuarios legítimos.

A. Productos afectados:

Esta vulnerabilidad afecta a los siguientes productos Cisco Meraki si ejecutan una versión vulnerable del firmware Cisco Meraki MX y tienen Cisco AnyConnect VPN con autenticación de certificado de cliente habilitada:

- MX64, MX65, MX67, MX68, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX400, MX450, MX600.
- MX64W, MX65W, MX67C, MX67W, MX68CW, MX68W.
- vMX.
- Z3, Z3C, Z4, Z4C.

Nota: Cisco AnyConnect VPN es compatible con los dispositivos Cisco Meraki MX y Cisco Meraki Z Series que ejecutan versiones de firmware de Cisco Meraki MX 16.2 y posteriores, excepto Cisco Meraki MX64 y MX65, que admiten Cisco AnyConnect VPN solo si ejecutan versiones de firmware de Cisco Meraki MX 17.6 y posteriores.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-sM5GCfm7

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°142	Fecha: 19-06-2025
		Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el software antivirus ClamAV		
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 escritura fuera de límites en el software antivirus ClamAV. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado provocar una condición de denegación de servicio (DoS) o ejecutar código arbitrario en el sistema objetivo.

2. DETALLES:

ClamAV es un motor antivirus de código abierto (open-source) diseñado para detectar y eliminar troyanos, virus, malware y otras amenazas maliciosas.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-20260 de tipo escritura fuera de límites en ClamAV, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema objetivo.

La vulnerabilidad existe debido a un error en los procesos de escaneo de PDF de ClamAV podría permitir que un atacante remoto no autenticado provoque un desbordamiento de búfer, una denegación de servicio (DoS) o ejecute código arbitrario en un dispositivo afectado.

Esta vulnerabilidad se debe a que los búferes de memoria se asignan incorrectamente al procesar archivos PDF. Un atacante podría explotar esta vulnerabilidad enviando un archivo PDF manipulado para que ClamAV lo escanee en un dispositivo afectado. Una explotación exitosa podría permitir al atacante provocar un desbordamiento de búfer, lo que probablemente resultaría en la finalización del proceso de escaneo de ClamAV y una DoS en el software afectado.

A. Productos afectados:

- ClamAV: 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, 1.0.5, 1.0.6, 1.0.7, 1.0.8, 1.1.0, 1.1.1, 1.1.2, 1.1.3, 1.2.0, 1.2.1, 1.2.2, 1.2.3, 1.3.0, 1.3.1, 1.3.2, 1.4.0, 1.4.1, 1.4.2.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://blog.clamav.net/2025/06/clamav-143-and-109-security-patch.html

Índice alfabético