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

# 126-2024-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°126 | Fecha: 30-05-2024 |
|---|---|---|
| | | Página: 4 de 9 |

| | | | |
|---|---|---|---|
| Componente que reporta | CENTRO NACIONAL DE SEGURIDAD DIGITAL | | |
| Nombre de la alerta | Cooler Master confirma que la información del cliente fue robada en una violación de datos | | |
| Tipo de Ataque | Robo de información | Abreviatura | RobInfo |
| Medios de propagación | Red, Internet, Redes sociales | | |
| Código de familia | K | Código de Sub familia | K01 |
| Clasificación temática familia | Uso inapropiado de recursos | | |

**Descripción**

## 1. ANTECEDENTES:

El fabricante de hardware informático Cooler Master ha confirmado que sufrió una violación de datos el 19 de mayo, lo que permitió a un actor de amenazas robar datos de clientes.

Cooler Master es un popular fabricante de hardware informático conocido por sus dispositivos de refrigeración, carcasas de computadora, fuentes de alimentación y otros periféricos.

## 2. DETALLES:

El sitio Fanzone de Cooler Master se utiliza para registrar la garantía de un producto, solicitar un RMA o abrir tickets de soporte, lo que requiere que los clientes completen datos personales, como nombres, direcciones de correo electrónico, direcciones, números de teléfono, fechas de nacimiento y direcciones físicas.

Un actor de amenazas conocido como 'Ghostr' indicó que pirateó el sitio web Fanzone de la compañía el 18 de mayo y descargaron sus bases de datos vinculadas.

Ghostr dijo que pudieron descargar 103 GB de datos durante la violación de Fanzone, incluida la información de más de 500.000 clientes.

El actor de amenazas también compartió muestras de datos, lo que permitió confirmar con numerosos clientes enumerados en la infracción que sus datos eran precisos y que recientemente solicitaron soporte o un RMA de Cooler Master. Además, uno de los archivos contiene alrededor de 1000 registros: se trata de llamadas recientes al servicio de soporte y solicitudes de devolución de productos.

Otros datos de las muestras incluían información del producto, información de los empleados e información sobre correos electrónicos con proveedores. El actor de amenazas afirmó tener información parcial de la tarjeta de crédito, pero no se pudo encontrar estos datos en las muestras de datos.

El actor de amenazas dice que venderán los datos filtrados en foros de piratería, pero no ha revelado el precio.

Si bien el actor de amenazas solo ha compartido una cantidad limitada de datos, si de hecho hay información sobre 500.000 clientes de Cooler Master, es muy probable que se venda a otro actor de amenazas.

Por lo tanto, todos los clientes de Cooler Master que hayan registrado una cuenta en el sitio Fanzone de la compañía deben estar atentos a los correos electrónicos de phishing dirigidos y otros ataques de ingenieros sociales diseñados para robar más información personal.

## 3. RECOMENDACIONES:

- Supervisar sus cuentas financieras por si hubiera alguna evidencia de fraude o suplantación de identidad.
- Practicar una higiene estricta de contraseñas. Utilizar contraseñas únicas para cada tarjeta y cambiarlas periódicamente.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Mantener el software actualizado. Actualizar periódicamente los sistemas operativos, las aplicaciones y el software de seguridad para corregir las vulnerabilidades.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

| | |
|---|---|
| Fuente de Información: | • hxxps://www.bleepingcomputer.com/news/security/cooler-master-confirms-customer-info-stolen-in-data-breach/ |

| | | |
|---|---|---|
| DINI | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°126 | Fecha: 30-05-2024<br>Página: 5 de 9 |

| | | | |
|---|---|---|---|
| Componente que reporta | DIRECCIÓN NACIONAL DE INTELIGENCIA | | |
| Nombre de la alerta | Vulnerabilidades críticas en el convertidor industrial de serie a Ethernet EDW-100 de Westermo | | |
| 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:

Nicolai Grødum y Sofia Lindqvist de PwC Noruega, han reportado dos vulnerabilidades de severidad **CRÍTICA** de tipo uso de contraseñas codificadas y credenciales insuficientemente protegidas que afectan al convertidor industrial de serie a Ethernet EDW-100 de Westermo. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto acceder al dispositivo utilizando credenciales codificadas y descargar nombres de usuario y contraseñas en texto sin cifrar.

## 2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-36080 de tipo uso de contraseñas codificadas, se debe a que el convertidor EDW-100 tiene una cuenta de administrador oculta con una contraseña codificada. En el paquete de firmware, en "image.bin", el nombre de usuario raíz y la contraseña de esta cuenta están codificados y expuestos como cadenas que pueden extraerse trivialmente. Actualmente no hay forma de cambiar esta contraseña.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-36081 de tipo credenciales insuficientemente en el convertidor EDW-100, podría permitir una solicitud GET no autenticada que puede descargar el archivo de configuración que contiene la configuración, el nombre de usuario y las contraseñas en texto sin cifrar.

### A. Productos afectados:

- Westermo EDW-100: todas las versiones.

## 3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.
- Implementar medidas como la segregación de la red, protección perimetral, protección de red a red y medidas de seguridad física. EDW-100 funciona como un convertidor industrial de serie a ethernet. Esto significa que el EDW-100 en sí mismo no tiene ninguna de las medidas de protección que requiere una postura de seguridad moderna; el EDW-100 no debe colocarse en el borde de la red, sino implementarse utilizando las técnicas mencionadas en el estándar IEC 62443.
- Tener habilitada la protección de red a red que, por ejemplo, se puede aplicar con una red privada virtual (VPN), en caso sea necesario que los datos entren o salgan de la zona de seguridad que contiene EDW-100.
- Contar con medidas de seguridad física, ya que la unidad puede ser vulnerable a ataques físicos y manipulaciones. Una recomendación para mitigar este riesgo es colocar la unidad en un recinto separado con cerraduras y alarmas que se activen si se abriera fuera del mantenimiento normal.

| | |
|---|---|
| Fuente de Información: | • hxxps://www.westermo.com/-/media/Files/Cyber-security/westermo_sa_EDW-100_24-05.pdf<br>• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-151-04 |

| | | |
|---|---|---|
| DINI | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°126 | Fecha: 30-05-2024<br>Página: 6 de 9 |

| | | | |
|---|---|---|---|
| Componente que reporta | DIRECCIÓN NACIONAL DE INTELIGENCIA | | |
| Nombre de la alerta | Vulnerabilidades en el sistema operativo central avanzado de A10 Networks | | |
| 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 reportado dos vulnerabilidades de severidad **ALTA** de tipo inyección de comando y asignación de permisos incorrecta en la interfaz gráfica de usuario (GUI) de administración de los sistemas del sistema operativo central avanzado (ACOS) de A10 Networks. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante local escalar privilegios y ejecutar código remoto arbitrario en instalaciones afectadas de A10 Thunder ADC.

## 2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-30368 de tipo inyección de comando, podría permitir a un atacante remoto ejecutar código arbitrario en instalaciones afectadas de A10 Thunder ADC. Se requiere autenticación para aprovechar esta vulnerabilidad. La falla específica existe dentro de la clase CsrRequestView. El problema se debe a la falta de validación adecuada de una cadena proporcionada por el usuario antes de usarla para ejecutar una llamada al sistema. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto de un usuario.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-30369 de tipo asignación de permisos incorrecta, podría permitir a un atacante local escalar privilegios en las instalaciones afectadas de A10 Thunder ADC. Un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema de destino para poder explotar esta vulnerabilidad. La falla específica existe dentro del instalador. El problema se debe a permisos incorrectos en un archivo. Un atacante puede aprovechar esta vulnerabilidad para escalar privilegios y ejecutar código arbitrario en el contexto de la raíz.

### A. Productos afectados:

- A10 Thunder ADC: versiones 4.1.4 – 4.1.4-GR1-P13, 5.1.0 – 5.2.1-P9 y 6.0.0 – 6.0.2-P1.

## 3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.
- Deshabilitar el servicio de administración de GUI, si no es necesario, para mitigar la exposición de un sistema ACOS afectado por esta vulnerabilidad. Se debe tener en cuenta que, al deshabilitar el servicio GUI de esta manera, también deshabilitará el servicio de administración de API RESTful de aXAPI para el sistema ACOS, lo que a su vez puede afectar las herramientas de administración central que utilizan el servicio aXAPI, incluidos los sistemas A10 aGalaxy y Harmony Controller.

| | |
|---|---|
| Fuente de Información: | • hxxps://support.a10networks.com/support/security_advisory/cve-2024-30368-cve-2024-30369 |

| | | |
|---|---|---|
| DINI | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°126 | Fecha: 30-05-2024<br>Página: 7 de 9 |

| | | | |
|---|---|---|---|
| Componente que reporta | DIRECCIÓN NACIONAL DE INTELIGENCIA | | |
| Nombre de la alerta | Actores de amenazas explotan vulnerabilidad critica en firewall de Palo Alto Networks | | |
| 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:

Los operadores del malware de minería de criptomonedas conocido como "RedTail" ha actualizado su arsenal de herramientas, incluyendo una vulnerabilidad de severidad **CRÍTICA** recientemente revelada que afecta los firewalls de Palo Alto Networks. Un ataque exitoso de explotación de esta vulnerabilidad crítica podría permitir a un atacante remoto no autenticado ejecutar código arbitrario con privilegios de root en el firewall de Palo Alto Networks.

## 2. DETALLES:

El grupo de ciberdelincuentes detrás del malware de minería de criptomonedas conocido como RedTail ha actualizado su arsenal de herramientas, incluyendo ahora una vulnerabilidad recientemente revelada que afecta los firewalls de Palo Alto Networks.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-3400 de tipo inyección de comando, podría permitir a un atacante no autenticado ejecutar código arbitrario con privilegios de root en el firewall PAN-OS 10.2, PAN-OS 11.0 y PAN-OS 11.1 de Palo Alto Networks. Una explotación exitosa es seguida por la ejecución de comandos diseñados para recuperar y ejecutar un script de shell bash desde un dominio externo que, a su vez, es responsable de descargar la carga útil de RedTail según la arquitectura de la CPU.

Otros mecanismos de propagación de RedTail implican la explotación de fallos de seguridad conocidos en los enrutadores TP-Link (CVE-2023-1389), ThinkPHP (CVE-2018-20062), Ivanti Connect Secure (CVE-2023-46805 y CVE-2024-21887). y VMWare Workspace ONE Access and Identity Manager (CVE-2022-22954).

Según los investigadores, los ciberdelincuentes han mejorado su malware con nuevas técnicas antianálisis, lo que representa un avance significativo en sus capacidades.

Asimismo, indicaron que, tras explotar la vulnerabilidad en PAN-OS, los atacantes ejecutan comandos para descargar y ejecutar un script de shell bash desde un dominio externo, el cual se encarga de descargar la carga útil de "RedTail", adaptándose a la arquitectura de la CPU del sistema comprometido.

Además de esta vulnerabilidad, "RedTail" también se propaga explotando fallas de seguridad conocidas en diversos dispositivos y plataformas, como los enrutadores TP-Link, ThinkPHP, Ivanti Connect Secure, y VMWare Workspace ONE Access and Identity Manager.

Cabe señalar que el malware "RedTail" fue documentado por primera vez en enero de 2024, destacando su uso de la vulnerabilidad Log4Shell para infectar sistemas Unix. En marzo de 2024, Barracuda Networks reveló que "RedTail" también se distribuía mediante la explotación de vulnerabilidades en SonicWall y Visual Tools DVR, además de ThinkPHP.

La última versión del malware, detectada en abril de 2024, incluye una configuración de minería cifrada y el uso del minero XMRig integrado, lo cual marca una evolución significativa en su sofisticación técnica. A diferencia de variantes anteriores, esta versión utiliza técnicas avanzadas de evasión y persistencia, bifurcándose varias veces para dificultar su análisis y eliminando cualquier instancia del GNU Debugger que encuentre.

A. **Indicadores de compromiso (IoC):**

Dominio:

- proxies[.]identitynetwork[.]top

IP:

- 92[.]118[.]39[.]120
- 193[.]222[.]96[.]163
- 79[.]110[.]62[.]25
- 68[.]170[.]165[.]36
- 193[.]222[.]96[.]163
- 94[.]156[.]79[.]60
- 94[.]156[.]79[.]129
- 185[.]216[.]70[.]138
- 78[.]153[.]140[.]51.

## 3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de firmware disponible que aborda esta vulnerabilidad.
- Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.
- Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.
- Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.
- Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.
- Bloquear los indicadores de compromisos (IOC) mostrados, en los dispositivos de seguridad de su infraestructura.

| | |
|---|---|
| **Fuente de Información:** | • hxxps://thehackernews.com/2024/05/redtail-crypto-mining-malware.html<br>• hxxps://security.paloaltonetworks.com/CVE-2024-3400<br>• hxxps://www.linkedin.com/feed/update/urn:li:activity:7151248530077044739/<br>• Equipo de Anti-Fraude y Dark Web Intelligence SecureSoft |

# Índice alfabético