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

129-2024-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°129	Fecha: 03-06-2024
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Malware de criptominería RedTail que explota la vulnerabilidad del 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:

Actualmente los actores de amenazas han incorporado una falla de seguridad recientemente revelada que afecta los firewalls de Palo Alto Networks. Siendo estos responsables del uso del malware de minería de criptomonedas “RedTail”.

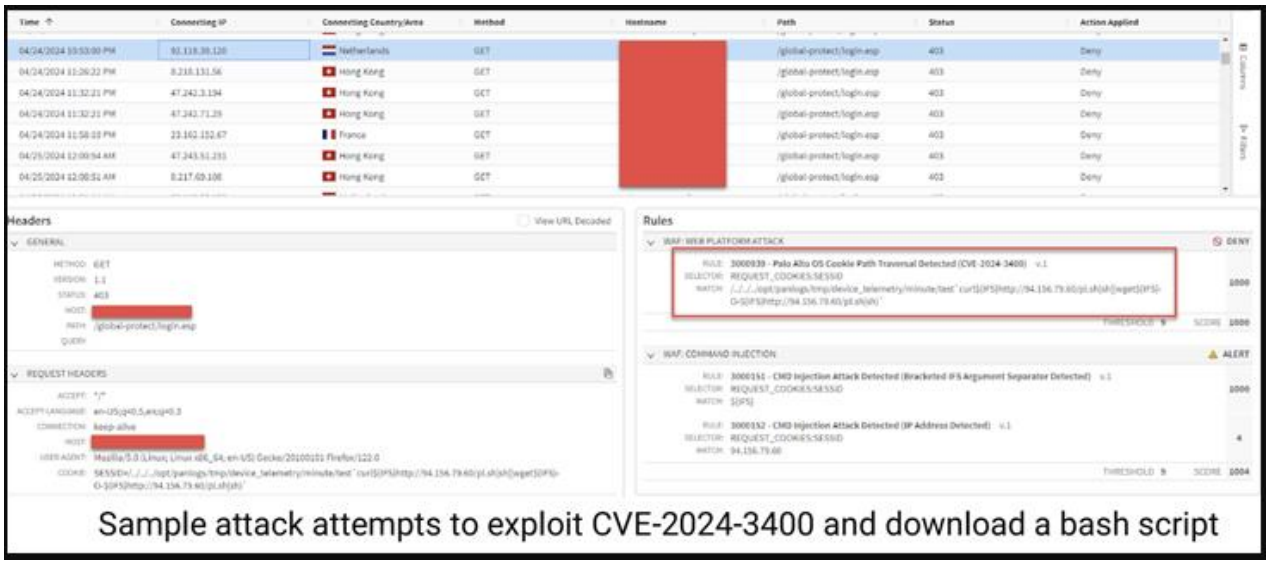
Palo Alto Networks es un fabricante de seguridad de redes de renombre mundial y PAN-OS es un sistema operativo desarrollado por Palo Alto Networks para sus dispositivos firewall.

2. DETALLES:

La secuencia de infección descubierta por Akamai explota una vulnerabilidad ya parcheada en PAN-OS rastreada como CVE-2024-3400 (puntuación CVSS: 10,0) que podría permitir a un atacante no autenticado ejecutar código arbitrario con privilegios de root en el firewall.

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 el payload RedTail basada en la arquitectura de la CPU.

La vulnerabilidad de día cero en los productos basados en PAN-OS de Palo Alto, publicada el 11 de abril de 2024, permite a los atacantes crear un archivo arbitrario que eventualmente posibilita la ejecución de comandos con privilegios de usuario root. Esta vulnerabilidad se explota al manipular el valor de la cookie SESSID, lo que induce a PAN-OS a crear un archivo con el nombre especificado en el valor de la cookie. Utilizando una técnica de recorrido de ruta, el atacante puede controlar tanto el nombre del archivo como el directorio en el que se almacena, lo que le da la capacidad de ejecutar código arbitrario con privilegios elevados. La vulnerabilidad está presente en la función GlobalProtect de ciertas versiones de PAN-OS.



Sample attack attempts to exploit CVE-2024-3400 and download a bash script

La puntuación CVSS de la vulnerabilidad es 10,0. En la actualidad, la prueba de concepto de esta vulnerabilidad se ha hecho pública y se ha descubierto que está en uso. Se recomienda a los usuarios pertinentes que tomen medidas de protección lo antes posible.

El malware puede extraer información sensible, lo que conduce a la violación de datos y a la pérdida potencial de propiedad intelectual.

Otro impacto se asocia a las interrupciones operativas. La actividad minera continua sobrecarga los recursos de la red, lo que puede provocar importantes tiempos de inactividad y reducir la eficacia operativa.

Además, las organizaciones pueden enfrentarse a importantes repercusiones financieras debido a los costes de reparación, los honorarios legales y las posibles multas reglamentarias en virtud del RGPD.

IoC

Puerta trasera de estilo upstyle:

- 3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac
- 5460b51da26c060727d128f3b3d6415d1a4c25af6a29fef4cc6b867ad3659078

Infraestructura de mando y control:

- 172.233.228[.]93
- hxxp://172.233.228[.]93/policy
- hxxp://172.233.228[.]93/patch
- 66.235.168[.]222

Puerta trasera de Python alojada:

- 144.172.79[.]92
- nhdata.s3-us-west-2.amazonaws[.]com

Versiones afectadas:

- PAN-OS 11.1 < 11.1.2-h3
- PAN-OS 11.0 < 11.0.4-h1
- PAN-OS 10.2 < 10.2.7-h8, < 10.2.8-h3, < 10.2.9-h1

3. RECOMENDACIONES:

- La solución principal consiste en actualizar urgentemente el software de PAN-OS a una de las nuevas versiones parcheadas que corrigen esta vulnerabilidad:

  PAN-OS 10.2
  - 10.2.9-h1 (Released 4/14/24)
  - 10.2.8-h3 (Released 4/15/24)
  - 10.2.7-h8 (Released 4/15/24)
  - 10.2.6-h3 (ETA: 4/16/24)
  - 10.2.5-h6 (ETA: 4/16/24)
  - 10.2.4-h16 (ETA: 4/19/24)
  - 10.2.3-h13 (ETA: 4/17/24)
  - 10.2.2-h5 (ETA: 4/18/24)
  - 10.2.1-h2 (ETA: 4/17/24)
  - 10.2.0-h3 (ETA: 4/18/24)

  PAN-OS 11.0
  - 11.0.4-h1 (Released 4/14/24)
  - 11.0.3-h10 (ETA: 4/16/24)
  - 11.0.2-h4 (ETA: 4/16/24)

- 11.0.1-h4 (ETA: 4/17/24)
- 11.0.0-h3 (ETA: 4/18/24)

PAN-OS 11.1

- 11.1.2-h3 (Released 4/14/24)
- 11.1.1-h1 (ETA: 4/16/24)
- 11.1.0-h3 (ETA: 4/17/24)

- Generar una regla personalizada para bloqueos de IOC's en perfiles entrantes perimetrales.
- Desconfiar de los correos alarmantes. Si un mensaje le indica o incentiva a tomar decisiones apresuradas o en un tiempo limitado, probablemente se trata de phishing.
- Disponer de sistemas antispam para correos electrónicos, de esta manera se reducen las posibilidades de infección a través de campañas masivas de spam por correo electrónico.
- Mantener una buena estrategia de respaldo de información: sistemas de copias de seguridad que deben estar aisladas de la red; y políticas de seguridad. Lo anterior permitirá neutralizar el ataque, restaurar las operaciones y evitar el pago del rescate. Gestionarlo con políticas de respaldo periódico que garanticen que se almacenará fuera de la red organizacional.
- Bloquear los ataques de esta vulnerabilidad mediante el identificador de amenaza 95187 (disponible en la versión de contenido de aplicaciones y amenazas 8833-8682 y posteriores), en caso que esté suscrito a Prevención de amenazas.
- Monitorear la red para detectar actividad anormal e investigar cualquier actividad inesperada que se presente.
- Realización periódica de evaluaciones de vulnerabilidad y pruebas de penetración.
- Garantizar la gestión oportuna de los parches para abordar las vulnerabilidades conocidas.
- Desplegar sistemas avanzados de detección de amenazas para controlar las actividades sospechosas.
- Educar a los empleados sobre las últimas técnicas de phishing y tácticas de ingeniería social, para reducir significativamente el riesgo de infiltración de malware.
- Tener un plan de respuesta a incidentes bien definido, el cual debe describir los pasos a seguir en caso de violación de la seguridad, garantizando una respuesta rápida y eficaz para mitigar los daños y restablecer la normalidad de las operaciones.
- Abrir un caso en el Portal de soporte técnico (CSP) y cargar un archivo de soporte técnico (TSF) para determinar si los registros de sus dispositivos coinciden con los indicadores de riesgo (IoC) conocidos para esta vulnerabilidad.
- Para obtener información actualizada sobre los productos y versiones afectados, consulte el aviso de seguridad de Palo Alto Networks sobre este problema en la última Fuente de Información.

Fuente de Información:	• hxxps://portal.cci-entel.cl/Threat_Intelligence/Boletines/1953/ • hxxps://nsfocusglobal.com/palo-alto-networks-pan-os-command-injection-vulnerability-cve-2024-3400/ • hxxps://enhacke.com/blog/malware-de-mineria-de-criptomonedas-redtail-aprovecha-la-vulnerabilidad-del-firewall-de-palo-alto-network-6659dcb54b38c • hxxps://hodeitek.com/es/blog/ciberseguridad/alerta-critica-redtail-miner-explota-la-vulnerabilidad-0-day-de-palo-alto-como-proteger-tu-empresa-en-la-ue/ • hxxps://unit42.paloaltonetworks.com/cve-2024-3400/ • hxxps://security.paloaltonetworks.com/CVE-2024-3400

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°129	Fecha: 03-06-2024 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de Inyección de código en la biblioteca Pdfmake		
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 una vulnerabilidad de severidad **alta** de tipo Inyección de código que afecta a la biblioteca Pdfmake. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La biblioteca Pdfmake es una herramienta de código abierto que permite generar documentos PDF de manera declarativa en JavaScript, tanto para uso en el lado del servidor como en el lado del cliente. Ofrece una amplia gama de características para personalizar la apariencia y estructura de los documentos PDF, incluyendo line-wrapping, alineaciones de texto, listas numeradas y bulleted, tablas y columnas, imágenes y gráficos vectoriales, estilos y márgenes, entre otras.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-25180 de tipo Inyección de código, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada incorrecta. Un atacante remoto puede enviar una solicitud POST especialmente diseñada al punto final /pdf y ejecutar código arbitrario en el sistema de destino.

NOTA: esto está en disputa porque el comportamiento del punto final /pdf es intencional. El punto final /pdf solo está disponible después de instalar un marco de prueba (que se encuentra fuera de la aplicación pdfmake). Cualquiera que instale esto es responsable de garantizar que solo esté disponible para evaluadores autorizados.

A. Productos afectados:

- Pdfmake: versión 0.2.9.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://github.com/joaoviictorti/My-CVES/blob/main/CVE-2024-25180/README.md • hxxp://www.youtube.com/watch?v=QcOlrWUGo6o • hxxp://security.snyk. io/vuln/SNYK-JS-PDFMAKE-6347243 • hxxp://github.com/bpampuch/pdfmake/issues/2702

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°129	Fecha: 03-06-2024 Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en el kernel de RedHat Linux		
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:

Red Hat Product Security ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo desreferencia del puntero NULL, lectura fuera de límites, uso después de la liberación y carreras de datos indata-races en el kernel de RedHat Linux. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto generar una condición de denegación de servicio (DoS) y elevación de privilegios en el sistema objetivo.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-2166 de tipo desreferencia del puntero NULL en el protocolo CAN en net/can/af_can.c en el kernel de Linux, donde es posible que ml_priv no se inicialice en la ruta de recepción de las tramas CAN. Esta falla permite que un usuario local bloquee el sistema o generar una condición de denegación de servicio.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-2176 de tipo lectura fuera de límites en compare_netdev_and_ip en drivers/infiniband/core/cma.c en RDMA en el kernel de Linux. Una limpieza inadecuada da como resultado una lectura fuera de límites. Esta falla permite que un usuario local falle o aumente sus privilegios en el sistema.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-52578 de tipo carrera de datos en la función, que fue informada por syzbot/KCSAN. Esta vulnerabilidad puede provocar comportamientos impredecibles, fallas o daños en la memoria, lo que potencialmente podría afectar el rendimiento de la red.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-1086 de tipo de uso después de la liberación en el componente netfilter: nf_tables del kernel de Linux puede explotarse para lograr una escalada de privilegios local. La función nft_verdict_init() permite valores positivos como error de eliminación dentro del veredicto del gancho y, por lo tanto, la función nf_hook_slow() puede causar una vulnerabilidad doblemente libre cuando NF_DROP se emite con un error de eliminación similar a NF_ACCEPT.

A. Productos afectados:

- Servidor Red Hat Enterprise Linux - AUS 8.2 x86_64.
- Servidor Red Hat Enterprise Linux: TUS 8.4 x86_64.
- Servidor Red Hat Enterprise Linux para Power LE - Servicios de actualización para soluciones SAP 8.4 ppc64le.
- Red Hat Enterprise Linux para x86_64: servicios de actualización para soluciones SAP 8.4 x86_64.
- Red Hat Enterprise Linux para tiempo real: servicio de actualización de telecomunicaciones 8.4 x86_64.
- Red Hat Enterprise Linux en tiempo real para NFV: servicio de actualización de telecomunicaciones 8.4 x86_64.

3. RECOMENDACIÓN:

- Actualizar los productos afectados con la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://access.redhat.com/errata/RHSA-2024:3528 • hxxps://access.redhat.com/errata/RHSA-2024:3529 • hxxps://access.redhat.com/errata/RHSA-2024:3530

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°129	Fecha: 03-06-2024 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en productos Baxter		
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:

Maarten Boone y Edwin Van Andel (CTO de Zerocopter) y Baxter han reportado dos vulnerabilidades de severidad **CRÍTICA** de tipo credenciales insuficientemente protegida y uso de clave criptográfica por defecto en varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto modificar la configuración del dispositivo y los datos del firmware, así como acceder a credenciales a usuarios no autorizados.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-5176 de tipo credenciales insuficientemente protegida se debe a que cualquier credencial que se haya utilizado para la autenticación o la entrada de datos durante el uso de la herramienta de configuración de Welch Allyn puede estar en peligro y debe cambiarse inmediatamente.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-5175 de tipo uso de clave criptográfica por defecto se debe a que el producto afectado utiliza una clave criptográfica predeterminada para una funcionalidad potencialmente crítica. Un atacante podría modificar las configuraciones del dispositivo y los datos del firmware, lo que podría afectar y/o retrasar la atención al paciente.

A. Productos afectados:

Los siguientes productos afectados de Baxter (anteriormente Hillrom y Welch Allyn) son:

- Welch Allyn Product Configuration Tool: versiones 1.9.4.1 y anteriores.
- Welch Allyn Connex Spot Monitor (CSM): versiones 1.52 y anteriores.

3. RECOMENDACIONES:

- Actualizar los productos afectados con la última versión de software disponible que aborda estas vulnerabilidades.
- Aplicar controles adecuados de seguridad física y de red.
- Comunicarse con el soporte técnico de Baxter o con su gerente de proyecto de Baxter para crear archivos de configuración, según sea necesario, ya que la herramienta de configuración de Welch Allyn se ha eliminado del acceso público.
- Configurar y aplicar una clave de cifrado única al producto (como se describe en el Manual de servicio de Connex Spot Monitor).

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-151-01 • hxxps://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-151-02

Índice alfabético