PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 06 de febrero de 2024

032-2024-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 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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°032	Fecha: 06-02-2024
		Página: 4 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Los Investigadores Revelan El Sofisticado Ransomware Utilizado Por Black Hunt		
Tipo de Ataque	Ransonware	Abreviatura	Ransonware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES**:

El ransomware Black Hunt se ha convertido recientemente en una amenaza importante para el panorama de la ciberseguridad. Este software malicioso ya ha causado estragos en alrededor de 300 empresas en Paraguay, provocando importantes daños e interrupciones en sus operaciones.

Es probable que el impacto de este ataque de ransomware sea de gran alcance y afecte no solo a las empresas afectadas sino también a sus clientes, empleados y otras partes interesadas.

En el año 2022, los investigadores de seguridad identificaron una nueva forma de ransomware conocida como Black Hunt.

2. **DETALLES:**

Este software malicioso está diseñado específicamente para atacar y comprometer diferentes tipos de sistemas operativos, poniendo en riesgo los datos y la privacidad de innumerables usuarios.

El famoso ransomware Black Hunt es conocido por utilizar técnicas avanzadas de cifrado de archivos para restringir el acceso a los datos de la víctima.

Este software malicioso también va un paso más allá y altera los nombres de los archivos afectados, dificultando a la víctima identificar y recuperar sus datos.

Según el análisis de Rapid7 , se ha descubierto que Black Hunt comparte ciertas similitudes con Lockbit, entre otros detalles técnicos.

Se sospecha que este software malicioso se desarrolló utilizando código filtrado del ransomware LockBit y tiene varias similitudes con el infame ransomware REvil .

Black Hunt cifra los archivos del sistema infectado y exige el pago de un rescate a cambio de la clave de descifrado.

Busca un archivo específico, "Vaccine.txt", en la ruta del directorio C:\ProgramData para determinar si el sistema ya se ha visto comprometido.

Esta cepa particular de ransomware tiene la capacidad de ocultar su ventana a la vista del usuario y modificar sus privilegios para operar de manera encubierta.

Además, tiene la capacidad de aceptar argumentos de línea de comandos, lo que permite una mayor personalización de su comportamiento.

La operación conocida como Black Hunt parece tener una lista predeterminada de países a los que apunta, y también parece tener una lista blanca de idiomas que puede utilizar para la ejecución.

El proceso implica la creación de entradas en el registro de la computadora para garantizar que el malware permanezca activo incluso después de reiniciar el sistema.

Además, el malware modifica la configuración de Windows para desactivar funciones de seguridad cruciales, dejando el sistema vulnerable a futuros ataques.

El ransomware utiliza la extensión de archivo “.Hunt2” para cifrar archivos y también elimina instantáneas.

El software malicioso intenta propagarse a otras computadoras de la red explotando vulnerabilidades en carpetas y archivos compartidos. Además, utiliza una variedad de técnicas para evitar la detección mediante medidas de seguridad.

3. RECOMENDACIONES:

- Practicar una higiene estricta de las contraseñas. Utilizar contraseñas únicas y complejas para todas las cuentas y cambiarlas periódicamente.
- Habilitar la autenticación de dos factores cuando esté disponible.
- No hacer clic en enlaces sospechosos ni descargue archivos adjuntos de fuentes desconocidas.
- Ejecutar la estrategia 3-2-1 de copias de seguridad, que consiste en realizar tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Mantener siempre actualizado los programas, tanto en los dispositivos como en los servidores, para evitar que los atacantes aprovechen las vulnerabilidades y se infiltren en su red.
- Utilizar un software antivirus confiable y mantenerlo activo y actualizado.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Procurar la gestión de un plan que incluya detección, investigación y respuesta a amenazas 24/7, ya sea internamente o en asociación con un proveedor especializado de servicios de detección y respuesta gestionadas.
- Contratar los servicios de una firma comprometida con la ciberseguridad, en donde, por ejemplo, tenga modelos de seguridad multicapa, y así asegure la infraestructura en varios niveles, incluyendo el físico, de red, de host y de aplicación.
- Contar con medidas eficaces de seguridad para mitigar riesgos y prevenir brechas y ataques de Ransomware.
- Trabajar en comunicaciones encriptadas, de modo tal que se protejan los datos en tránsito. Esto incluye el uso de protocolos como HTTPS para interfaces web, SSL/TLS para la comunicación entre componentes y soluciones de almacenamiento encriptado.
- Realizar una Gestión de Identidad y Acceso (IAM), que asegure que los usuarios tengan permisos apropiados para acceder a recursos. Esto ayuda a prevenir el acceso no autorizado y la escalada de privilegios.
- En caso de infección, no pagar el rescate ni contactar con los ciberdelincuentes, ya que no hay garantía de que cumplan sus promesas. En su lugar, buscar ayuda profesional para eliminar el ransomware y restaurar los archivos cifrados.

Fuente de Información:	• hxxps://gbhackers.com/black-hunt-ransomware-attack/#google_vignette • hxxps://penguin.digital/es-news-posts/ransomware-black-hunt-como-procede-este-software-malicioso-y-como-podemos-protegernos-de-el-en-paraguay

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°032**	**Fecha: 06-02-2024** **Página: 6 de 11**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de omisión de la política de control de acceso Snort 3 de varios 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 ha reportado una vulnerabilidad de severidad **MEDIA** de tipo omisión de la política de control de acceso que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir las políticas configuradas en un sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-20246 de tipo omisión de la política de control de acceso que afectan a múltiples de sus productos en las políticas de control de acceso de Snort, podría permitir que un atacante remoto no autenticado eluda las políticas configuradas en un sistema afectado.

Esta vulnerabilidad se debe a un error lógico que ocurre cuando se completan las políticas de control de acceso. Un atacante podría aprovechar esta vulnerabilidad estableciendo una conexión con un dispositivo afectado. Un exploit exitoso podría permitir al atacante eludir las reglas de control de acceso configuradas en el sistema afectado.

A. Productos afectados:

- Open Source Snort 3.
- Cisco Firepower Threat Defense (FTD) y Cisco FirePOWER Services, cuando ejecutan Snort 3.
- Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del motor Snort Intrusion Prevention System (IPS) de Cisco Unified Threat Defense (UTD) para el software Cisco IOS XE o del motor Cisco UTD para Cisco IOS XE SD.
- Esta vulnerabilidad afecta a Cisco Umbrella Secure Internet Gateway (SIG), que está basado en la nube.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.
- Usar la herramienta Cisco Software Checker que Cisco ha proporcionado, para que los clientes puedan determinar si han sufrido exposición a las vulnerabilidades en el software Cisco ASA, FMC y FTD. Esta herramienta identifica cualquier aviso de seguridad de Cisco que afecte una versión de software específica y la versión más temprana que soluciona las vulnerabilidades que se describen en cada aviso (“Primera solución”).

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort3acp-bypass-3bdR2BEh

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°032**	**Fecha: 06-02-2024**
		Página: 7 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en Western Digital MyCloud PR4100		
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 **MEDIA** de tipo consumo incontrolado de recursos en un punto final y falsificación de solicitudes del lado del servidor en Western Digital MyCloud PR4100. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto crear una condición de denegación de servicio en las instalaciones afectadas de dispositivos NAS Western Digital MyCloud PR4100.

2. DETALLES:

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-22819 podría permitir a un atacante remoto crear una condición de denegación de servicio en las instalaciones afectadas de dispositivos NAS Western Digital MyCloud PR4100. No se requiere autenticación para aprovechar esta vulnerabilidad. La falla específica existe dentro del servidor RESTSDK. El problema se debe al consumo incontrolado de recursos. Un atacante puede aprovechar esta vulnerabilidad para crear una condición de denegación de servicio en el dispositivo.

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-22817 podría permitir a un atacante adyacentes a la red ejecutar código arbitrario en instalaciones afectadas de dispositivos NAS Western Digital MyCloud PR4100. No se requiere autenticación para aprovechar esta vulnerabilidad. La falla específica existe dentro del servidor RESTSDK. El problema se debe a la falta de validación adecuada de un URI antes de acceder a los recursos. Un atacante puede aprovechar esto junto con otras vulnerabilidades para ejecutar código arbitrario en el contexto de la raíz.

A. Productos afectados:

- Western Digital MyCloud PR4100.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que Western Digital ha publicado para abordar estas vulnerabilidades.

Fuente de Información:	• hxxps://www.westerndigital.com/support/product-security/wdc-24001-western-digital-my-cloud-os-5-my-cloud-home-duo-and-sandisk-ibi-firmware-update

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°032	Fecha: 06-02-2024
		Página: 8 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en Http File Server de Rejetto		
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 neutralización inadecuada de secuencias CRLF (inyección CRLF) y redirección de URL a un sitio que no es de confianza (Redirección abierta) en Http File Server de Rejetto. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante realizar un ataque de secuencias de comandos entre sitios y ataques de envenenamiento de caché.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-1226 de tipo uso neutralización inadecuada de secuencias CRLF, señala que la inclusión de datos invalidados en un encabezado HTTP permite a un atacante especificar la respuesta HTTP completa representada por el navegador. Un atacante podría controlar la respuesta y elaborar ataques como secuencias de comandos entre sitios y ataques de envenenamiento de caché.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-1227 de tipo redirección de URL a un sitio que no es de confianza, cuya explotación podría permitir a un atacante crear una dirección URL personalizada y redirigir una página legítima a un sitio malicioso. Esta vulnerabilidad señala que una aplicación web acepta una entrada controlada por el usuario que especifica un enlace a un sitio externo y utiliza ese enlace en un redireccionamiento. Esto simplifica los ataques de phishing.

A. Productos afectados:

- Http File Server versión 2.2a, build #124.

3. RECOMENDACIÓN:

- Actualizar el producto afectado versiones posteriores donde la vulnerabilidad ha sido solucionada. La versión afectada no está soportada en la actualidad.

Fuente de Información:	• hxxps://www.rejetto.com/hfs/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°032**	**Fecha: 06-02-2024**
		Página: 9 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en TP-Link Omada ER605		
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 desbordamiento de búfer basado en la pila en TP-Link Omada ER605. La explotación exitosa de esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-1179 de tipo desbordamiento de búfer basado en la pila, existe debido a un error de límite en el manejo de las opciones de DHCP. Un atacante remoto en la red local puede provocar un desbordamiento de búfer basado en pila y ejecutar código arbitrario en el sistema de destino.

A. Productos afectados:

- Omada ER605: antes de 2_2.2.4 compilación 20240119.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://www.zerodayinitiative.com/advisories/ZDI-24-085/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°032	Fecha: 06-02-2024
		Página: 10 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en B&R Automation		
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:

Centro de Garantía de Seguridad de Dispositivos de ABB ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo uso de un algoritmo criptográfico roto o arriesgado en B&R Automation. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante, no autenticado, ejecutar ataques de *Man-in* the-Middle (MITM), o descifrar las comunicaciones entre los productos afectados y otras partes.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-0323 de tipo uso de un algoritmo criptográfico roto o arriesgado, señala que un atacante, no autenticado, con acceso a la red que consiguiese explotar esta vulnerabilidad, podría ejecutar ataques Man-int-he-Middle o descifrar las comunicaciones entre los productos afectados y otras partes. Esta vulnerabilidad, utiliza un algoritmo o protocolo criptográfico defectuoso o riesgoso.

A. Productos afectados:

- B&R Automation Runtime, versiones anteriores a I4.93.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.br-automation.com/fileadmin/SA23P004_FTP_uses_unsecure_encryption_mechanisms-f57c147c.pdf

Índice alfabético