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

106-2024-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°106	Fecha: 07-05-2024
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El Nuevo Ataque TunnelVision Permite A Los Atacantes Espiar El Tráfico VPN		
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:

Utilizar una VPN, es una de las opciones para navegar con mayor privacidad por la red. El problema llega cuando hay un fallo con ese programa, dispositivo o incluso sistema. Si la información se filtra en la red, la privacidad está en peligro.

En un descubrimiento innovador, los expertos en ciberseguridad de Leviathan Security Group han revelado un nuevo tipo de ciberataque denominado "TunnelVision", que representa una amenaza para la seguridad de las redes privadas virtuales (VPN). Ha sido registrada la vulnerabilidad como CVE-2024-3661.

2. DETALLES:

Se debe tener en cuenta que no se ha logrado romper el protocolo criptográficamente seguro de una VPN, por lo que sigue funcionando correctamente. Sin embargo, lo que hace es evitar el cifrado de la VPN y un atacante podría forzar que la navegación salga fuera del túnel VPN. Para ello utilizan funciones que están integradas en DHCP. Alguien que se aproveche de este fallo podría espiar la navegación.

Este tipo de ataque lo han denominado Decloaking. Es necesario que el atacante esté en la misma red y, a partir de ahí, convertirse en su servidor DHCP fraudulento, aprovecharse de la falsificación de ARP e interceptar el tráfico entre el verdadero DHCP y el cliente, utilizando la opción 121 de DHCP para establecer una ruta en la tabla de enrutamiento del usuario de VPN. Precisamente la opción 121 permite a los administradores agregar rutas estáticas sin clases a las tablas de enrutamiento del cliente.

Básicamente, se configura el DHCP para que se utilice como puerta de enlace, de tal manera que, cuando el tráfico llega a nuestra puerta de enlace, se utilizan reglas de reenvío de tráfico en el servidor DHCP para pasar el tráfico a una puerta de enlace legítima mientras se espían la información, impulsando rutas para las cuales no actúa la interfaz virtual de la VPN y no llega a cifrarlas.

El ataque puede ser llevado a cabo de manera más efectiva por una persona que tenga control administrativo sobre la red a la que se conecta el objetivo. En ese escenario, el atacante configura el servidor DHCP para usar la opción 121. También es posible que las personas que pueden conectarse a la red como usuarios sin privilegios realicen el ataque configurando su propio servidor DHCP no autorizado.

Para empeorar las cosas, el problema está relacionado con DHCP, lo que significa que no importa qué VPN se esté utilizando o en qué sistema operativo se esté ejecutando: probablemente seas vulnerable.

"Además, la potencia del algoritmo de cifrado que utiliza una VPN no hace ninguna diferencia", señaló Leviathan Security. "El efecto de TunnelVision es independiente del protocolo VPN subyacente porque reconfigura la pila de red del sistema operativo en la que se basa la VPN".

Curiosamente, Android es el único sistema operativo que inmuniza completamente a las aplicaciones VPN contra el ataque porque no implementa la opción 121. Para todos los demás sistemas operativos, no existen soluciones completas. Cuando las aplicaciones se ejecutan en Linux, hay una configuración que minimiza los efectos, pero incluso entonces, TunnelVision se puede utilizar para explotar un canal lateral que se puede utilizar para anonimizar el tráfico de destino y realizar ataques dirigidos de denegación de servicio.

Para explotar el cliente VPN de alguien se deben cumplir lo siguiente:

El atacante debe estar en la misma red local que el host objetivo.

El host objetivo debe aceptar una concesión DHCP del servidor controlado por el atacante.

El cliente DHCP del host de destino debe implementar la opción 121 de DHCP.

3. RECOMENDACIONES:

- Ejecutar la VPN dentro de una máquina virtual cuyo adaptador de red no esté en modo puente.
- Conectar la VPN a Internet a través de la red Wi-Fi de un dispositivo celular.
- Utilizar puntos de acceso. Se trata de redes Wi-Fi temporales que van a estar controladas con un dispositivo móvil. Esto requiere de una contraseña, por lo que el atacante debería tener problemas para acceder a la red local.
- No utilizar redes que no sean de confianza (Wi-Fi público).
- Implementar medidas para detectar y bloquear servidores DHCP no autorizados.
- Habilitar espacios de nombres de red, para los usuarios de linux.
- Instar a los fabricantes de sistemas operativos, que no son Linux, a implementar espacios de nombres de red.
- Actualizar periódicamente el software VPN: asegurarse de que el software de su cliente y servidor VPN esté actualizado con los últimos parches y actualizaciones de seguridad.
- Monitorear el tráfico de la red, implementando herramientas y prácticas en busca de actividades inusuales que puedan indicar una posible infracción.

Fuente de Información:	• hxxps://gbhackers.com/new-tunnelvision-attack-lets/ • hxxps://testdevelocidaddeinternet.es/tecnologia/un-nuevo-ataque-contra-practicamente-todas-las-aplicaciones-vpn-neutraliza-todo-su-proposito/ • hxxps://seguridad.cicese.mx/noticia/2232/Todas-las-VPN-en-jaque,-este-grave-fallo-de-diseño-permite-evitar-el-cifrado-del-tráfico • hxxps://www.theregister.com/2024/05/07/vpn_tunnelvision_dhcp/ • hxxps://www.leviathansecurity.com/blog/tunnelvision

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°106	Fecha: 07-05-2024
		Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en dispositivos de la serie NPort 5100A de MOXA		
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 Cross-Site Scripting (XSS) que afecta a los dispositivos de la serie NPort 5100A de MOXA. La explotación exitosa de estas vulnerabilidades podría permitir a un usuario malintencionado inyectar scripts del lado del cliente en páginas web vistas por otros usuarios. Un atacante podría aprovechar esto para obtener información confidencial y escalar privilegios.

2. DETALLES:

El NPort 5100A es un dispositivo de servidor de dispositivo serie de red fabricado por Moxa. Este dispositivo permite conectar dispositivos serie RS-232/422/485 a una red Ethernet para facilitar la comunicación en entornos industriales. usuarios malintencionados inyectar scripts del lado del cliente en páginas web vistas por otros usuarios. Un atacante podría aprovechar esto para robar información confidencial o escalar privilegios.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-3576 en el firmware v1.6 de la serie NPort 5100A y versiones anteriores se ven afectadas por la vulnerabilidad XSS del servidor web. La vulnerabilidad se debe a que no se neutralizan correctamente las entradas controlables por el usuario antes de colocarlas en la salida. Los usuarios malintencionados pueden utilizar la vulnerabilidad para obtener información confidencial y escalar privilegios. Un ataque XSS exitoso podría permitir a un atacante: Robar cookies de sesión y secuestrar sesiones de usuario, desfigurar sitios web, realizar ataques de phishing, instalar malware o redirigir a los usuarios a sitios maliciosos. Un ataque exitoso podría provocar robo de datos, destrucción de sitios web, infecciones de malware y otros ataques contra usuarios de los dispositivos NPort afectados.

A. Productos afectados:

- Serie NPort 5100A, versión de firmware v1.6 y versiones anteriores.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la serie NPort 5100A versión 1.6 o posterior para abordar esta vulnerabilidad.
- Minimizar la exposición de la red para garantizar que no se pueda acceder al dispositivo desde Internet.
- Utilizar métodos seguros, como redes privadas virtuales (VPN), en caso se requiera acceso remoto.
- Desactivar el servicio web temporalmente, si completó la configuración para evitar daños mayores, debido a estas vulnerabilidades hasta que se instale el parche o se actualice el firmware.

Fuente de Información:	• hxxps://www.moxa.com/en/support/product-support/security-advisory/mpsa-246328-nport-5100a-series-store-xss-vulnerability • hxxps://www.moxa.com/en/support/product-support/security-advisory/nport-5100a-series-serial-device-servers-vulnerability-(1) • hxxps://www.cve.org/CVERecord?id=CVE-2024-3576

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°106	Fecha: 07-05-2024
		Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades críticas en Delta Electronics DIAEnergie		
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 múltiples vulnerabilidades de severidad **ALTA** de tipo inyección SQL y error de validación de entrada que afecta a DIAEnergie de Delta Electronics. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar consultas SQL arbitrarias en la base de datos. Asimismo, un atacante remoto realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-4547 de tipo inyección SQL, podría permitir a un atacante remoto ejecutar consultas SQL arbitrarias en la base de datos, la vulnerabilidad existe debido a una limpieza insuficiente de los datos proporcionados por el usuario cuando CEBC.exe procesa un mensaje "RecalculateScript". Un atacante remoto puede enviar una solicitud especialmente diseñada a la aplicación afectada y ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación. La explotación exitosa de esta vulnerabilidad puede permitir a un atacante remoto leer, eliminar, modificar datos en la base de datos y obtener control total sobre la aplicación afectada.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-4548 de tipo inyección SQL, podría permitir a un atacante remoto ejecutar consultas SQL arbitrarias en la base de datos, la vulnerabilidad existe debido a una limpieza insuficiente de los datos proporcionados por el usuario cuando CEBC.exe procesa un mensaje "RecalculateHDMWYC". Un atacante remoto puede enviar una solicitud especialmente diseñada a la aplicación afectada y ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación. La explotación exitosa de esta vulnerabilidad puede permitir a un atacante remoto leer, eliminar, modificar datos en la base de datos y obtener control total sobre la aplicación afectada.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-4549 de tipo error de validación de entrada, podría permitir a un atacante remoto realizar un ataque de DoS. La vulnerabilidad existe debido a una validación insuficiente de la entrada proporcionada por el usuario al procesar un "¡Reinicio de ICS!" mensaje. Un atacante remoto puede pasar entradas especialmente diseñadas a la aplicación y realizar un ataque de DoS.

A. Productos afectados:

- DIAEnergía: 1.10.1.8610.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://www.tenable.com/security/research/tra-2024-13

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°106	Fecha: 07-05-2024 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en Google Chrome		
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 uso después de la liberación y desbordamiento de búfer basado en montón que afecta al navegador Google Chrome. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino y comprometer el sistema vulnerable.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-4558 de tipo uso después de la liberación, existe debido a un error de uso después de la liberación dentro del componente ANGLE en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, provocar un error de uso después de la liberación y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de la vulnerabilidad puede permitir que un atacante comprometa el sistema vulnerable.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-4559 de tipo desbordamiento de búfer basado en montón, existe debido a un error de límite al procesar contenido HTML que no es de confianza en WebAudio. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la abra, provocar un desbordamiento de búfer basado en el montón y ejecutar código arbitrario en el sistema de destino.

A. Productos afectados:

- Google Chrome: 100.0.4896.60 - 124.0.6367.119.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_7.html • hxxps://issues.chromium.org/issues/337766133

Índice alfabético