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

199-2024-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°199	Fecha: 28-08-2024 Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Medidas que se deben tomar al compartir el DNI		
Tipo de Ataque	Suplantación	Abreviatura	Suplantación
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G02
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

En la actualidad, existen numerosas situaciones en las que nos vemos obligados a compartir nuestro Documento Nacional de Identidad (DNI). Desde la firma de contratos hasta la inscripción en cursos online pasando por la reserva de alojamientos o la cumplimentación de trámites, son muchos los casos en los que es necesario aportar el DNI para verificar nuestra identidad. No obstante, puede acarrear graves riesgos y causar serios problemas, como el robo de identidad, el fraude u otros delitos cibernéticos, por lo que es necesario tomar ciertas precauciones para evitar complicaciones y proteger nuestra información personal.

2. DETALLES:

Muchos negocios incursionan en el comercio electrónico y adoptan protocolos para garantizar que la entrega física de sus productos se realiza de manera segura. En ese proceso, algunas empresas estarían exigiendo a los clientes el envío de una fotografía de su Documento Nacional de Identidad (DNI), a fin de cerciorarse que la entrega del bien se efectúa al verdadero comprador.

Al respecto, la ANPD (Autoridad Nacional de Protección de Datos) del Ministerio de Justicia y Derechos Humanos (MINJUSDH) recuerda a la ciudadanía que, de acuerdo al principio de proporcionalidad recogido en la Ley de Protección de Datos Personales (Ley N°29733), para la compra y venta de productos solo deben solicitarse los datos estrictamente necesarios para efectuar la entrega del bien. Cualquier procesamiento de datos personales debe ser pertinente, apropiado y no exceder el propósito para el cual se recopilaron inicialmente.

En ese sentido, la ANPD advierte que la captura fotográfica del DNI implica el otorgamiento de datos personales que no resultan relevantes para la entrega; tales como la fecha de nacimiento, el estado civil, el dígito de verificación o el ubigeo. Es importante advertir esto puede traerte muchos problemas, ya que el DNI, en su versión azul y electrónica, guarda códigos y cifras sensibles que solo el titular debe poseer.

Una de las consecuencias de brindar esta fotografía es la suplantación de identidad. Los delincuentes pueden usarla para la creación de documentos falsos o modificar documentos existentes, haciéndose pasar por ti para realizar actividades ilegales como fraudes financieros o incluso delitos más graves.

Además, con el retrato de tu DNI, los delincuentes podrían tratar de abrir cuentas bancarias, solicitar tarjetas de crédito o inscribirse en servicios en línea bajo tu identidad, lo que podría resultar en la acumulación de deudas a tu nombre y dañar tu historial crediticio.

3. RECOMENDACIONES:

- Enviar la imagen del DNI en blanco y negro para que sea más evidente que es una fotocopia.
- Pixelar los datos que no sean necesarios, entre ellos es especialmente importante la firma.
- Escribir un texto sobre la fotografía del DNI que detalle el motivo por el que se comparte.

Fuente de Información:	• hxxps://larepublica.pe/sociedad/2024/03/27/por-que-no-deberias-enviar-la-foto-de-tu-dni-por-redes-sociales-y-que-pasa-si-lo-haces-reniec-atmp-2178954 • hxxps://www.gob.pe/institucion/minjus/noticias/294698-fotografiar-un-dni-comorequisito-para-la-entrega-de-un-producto-adquirido-via-online-genera-riesgos-altitular-de-los-datos-personales • hxxps://www.escudodigital.com/ciberseguridad/policia-nacional-advierte-tres-medidas-deben-tomar-compartir-dni_60181_102.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°199	Fecha: 28-08-2024 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el agente de retransmisión DHCPv6 del software Cisco NX-OS		
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 **ALTA** de tipo desreferencia de puntero NULL en el agente de retransmisión DHCPv6 del software Cisco NX-OS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado generar una condición de denegación de servicio (DoS) en un dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-20446 de tipo desreferencia de puntero NULL en el agente de retransmisión DHCPv6 del software Cisco NX-OS, podría permitir que un atacante remoto no autenticado genere una condición de DoS en un dispositivo afectado.

Esta vulnerabilidad se debe a un manejo inadecuado de campos específicos en un mensaje RELAY-REPLY de DHCPv6. Un atacante podría aprovechar esta vulnerabilidad enviando un paquete DHCPv6 diseñado a cualquier dirección IPv6 que esté configurada en un dispositivo afectado. Una explotación exitosa podría permitir al atacante provocar que el proceso dhcp_snoop se bloquee y se reinicie varias veces, lo que hace que el dispositivo afectado se recargue y genere una condición de DoS.

A. Productos afectados:

Esta vulnerabilidad afecta a los Switches Cisco Nexus de las series 3000 y 7000 y a los Switches Nexus de la serie 9000 en modo NX-OS independiente si se cumplen todas las condiciones siguientes:

- Están ejecutando el software Cisco NX-OS versión 8.2(11), 9.3(9) o 10.2(1).
- Tienen habilitado el agente de retransmisión DHCPv6.
- Tienen al menos una dirección IPv6 configurada en el dispositivo.

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-nxos-dhcp6-relay-dos-znEAA6xn • hxxps://cve.org/CVERecord?id=CVE-2024-20446

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°199	Fecha: 28-08-2024 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Netfilter Conntrack del kernel de 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:

Se ha reportado una vulnerabilidad de severidad **MEDIA** de tipo confusión de tipos en Netfilter Conntrack del kernel de Linux. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante ejecutar código arbitrario y divulgar información confidencial sobre las instalaciones afectadas del kernel de Linux.

2. DETALLES:

Netfilter Conntrack: Conntrack-tools es un conjunto de herramientas de espacio de usuario de software libre para Linux que permiten a los administradores de sistemas interactuar con el Sistema de seguimiento de conexión, que es el módulo que proporciona inspección de paquetes con estado para iptables.

La vulnerabilidad de severidad **media** de tipo confusión de tipos en Netfilter Conntrack del kernel de Linux, podría permitir a un atacante local divulgar información confidencial sobre las instalaciones afectadas del kernel de Linux. Para explotar esta vulnerabilidad, un atacante primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema de destino.

La falla específica existe en la implementación del seguimiento de conexiones. El problema surge de la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede generar una condición de confusión de tipos. Un atacante puede aprovechar esto junto con otras vulnerabilidades para ejecutar código arbitrario en el contexto del núcleo.

A. Productos afectados:

- Netfilter Conntrack del kernel de Linux.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://patchwork.kernel.org/project/netdevbpf/patch/20240717215214.225394-2-pablo@netfilter.org/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°199	Fecha: 28-08-2024 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	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 confusión de tipos y escritura fuera de límites en Google Chrome V8. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto explotar la corrupción de heap a través de una página HTML especialmente diseñada.

2. **DETALLES:**

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-7971 de tipo confusión de tipos en V8 en Google Chrome V8, podría permitir a un atacante remoto explotar la corrupción de heap a través de una página HTML manipulada.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-7965 de tipo escritura fuera de límites en V8 en Google Chrome V8, podría permitir a un atacante remoto explotar potencialmente la corrupción de heap a través de una página HTML manipulada.

A. **Productos afectados:**

- Google Chrome, anteriores a la versión128.0.6613.84.

3. **RECOMENDACIÓN:**

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

Fuente de Información:	• hxxps://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html • hxxps://issues.chromium.org/issues/360700873 • hxxps://issues.chromium.org/issues/356196918

Índice alfabético