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

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 04 de mayo de 2022

N° 122-2022-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

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 122**	**Fecha: 04-05-2022**
		Página 4 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en biblioteca estándar de C que afecta a productos IoT		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

Investigadores de Nozomi Networks Labs, han descubierto una vulnerabilidad de severidad CRÍTICA que afecta la implementación del Sistema de Nombres de Dominio (DNS) de todas las versiones de las bibliotecas para el lenguaje de programación C, "uClibc" y "uClibc-ng", que se usa comúnmente en la creación de software para productos (IoT). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto realizar ataques de envenenamiento de DNS. Un atacante podría robar y/o manipular la información transmitida por los usuarios y realizar otros ataques contra esos dispositivos para comprometerlos por completo.

2. Detalles:

- uClibc es una biblioteca C para desarrollar sistemas Linux integrados y es utilizado por los principales proveedores, como Linksys, Netgear y Axis, y distribuciones de Linux como Embedded Gentoo. La biblioteca uClibc-ng es una bifurcación diseñada específicamente para OpenWRT, un sistema operativo común para enrutadores probablemente implementado en varios sectores de infraestructura crítica.
- Nozomi descubrió la vulnerabilidad (registrada bajo ICS-VU-638779, VU#473698) que afecta a la implementación DNS de todas las versiones de las bibliotecas para el lenguaje de programación C uClibc y uClibc-ng en productos IoT. La vulnerabilidad se debe por la previsibilidad de los ID de transacción incluidos en las solicitudes de DNS generadas por la biblioteca, lo que podría permitir a un atacante realizar ataques de envenenamiento de DNS contra el dispositivo de destino.
- En un ataque de envenenamiento de DNS, un atacante puede engañar a un cliente de DNS para que acepte una respuesta falsificada, lo que induce a cierto programa a realizar comunicaciones de red con un punto final definido arbitrariamente, y no con el legítimo. Un ataque de envenenamiento de DNS puede permitir a un atacante realizar un ataque posterior de Man-in-the-Middle, al envenenar los registros de DNS, y redirigir las comunicaciones de red a un servidor bajo su control. El atacante podría robar y/o manipular la información transmitida por los usuarios y realizar otros tipos de ataques contra estos dispositivos y comprometerlos por completo.
- Nozomi Networks señalo que tiene un interés particular en el error porque la biblioteca uClibc-ng está diseñado para OpenWRT. El Proyecto OpenWRT es un sistema operativo Linux dirigido a dispositivos integrados e implementado en varios sectores de infraestructura crítica.
- Nozomi dijo, además, que la interacción de los dispositivos IoT con la tecnología ICS tradicional ha llamado más la atención en los últimos años, ya que la industria y el gobierno han prestado más atención a las amenazas cibernéticas contra la infraestructura crítica.

3. Productos afectados:

- Biblioteca C uClibc;
- Biblioteca C Integrada uClibc-ng.

4. Solución:

- Nozomi Networks, indico que esta vulnerabilidad permanece sin parchear, sin embargo, se encuentran trabajando junto con el mantenedor de la biblioteca y la comunidad en general para encontrar una solución.

Fuentes de información	▪ hxxps://therecord.media/iot-vulnerability-ics-nozomi-networks-uclibc-ng/?web_view=true ▪ hxxps://www.nozominetworks.com/blog/nozomi-networks-discovers-unpatched-dns-bug-in-popular-c-standard-library-putting-iot-at-risk/ ▪ hxxps://www.uclibc-ng.org/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 122	Fecha: 04-05-2022
		Página 5 de 8

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en Cisco Enterprise NFVIS		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

Cisco ha reportado múltiples vulnerabilidades de severidad CRÍTICA de tipo control de acceso inadecuado y restricción incorrecta de la referencia de entidad externa XML en Cisco Enterprise NFV Infrastructure Software (NFVIS). La explotación exitosa de estas vulnerabilidades podría permitir que un atacante remoto no autenticado escape de la máquina virtual invitada (VM) a la máquina host, inyecte comandos que se ejecutan en el nivel raíz o filtre datos del sistema desde el host a cualquier máquina virtual configurada.

2. Detalles:

- La vulnerabilidad crítica identificada como CVE-2022-20777 en la función Entrada/Salida de próxima generación (NGIO) de Cisco Enterprise NFVIS podría permitir que un atacante remoto autenticado escape de la máquina virtual invitada para obtener acceso no autorizado a nivel raíz en el host NFVIS. Esta vulnerabilidad se debe a restricciones de invitados insuficientes. Un atacante podría explotar esta vulnerabilidad enviando una llamada API desde una máquina virtual que se ejecutará con privilegios de nivel raíz en el host NFVIS. Una explotación exitosa podría permitir que el atacante comprometiera completamente el host NFVIS.
- La vulnerabilidad de severidad alta identificada como CVE-2022-20779 en el proceso de registro de imágenes de Cisco Enterprise NFVIS podría permitir que un atacante remoto no autenticado inyecte comandos que se ejecutan en el nivel raíz en el host NFVIS durante el proceso de registro de imágenes. Esta vulnerabilidad se debe a una validación de entrada incorrecta. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un administrador en la máquina host para que instale una imagen de VM con metadatos manipulados que ejecutará comandos con privilegios de nivel raíz durante el proceso de registro de VM. Una explotación exitosa podría permitir que el atacante inyecte comandos con privilegios de nivel raíz en el host NFVIS.
- La vulnerabilidad de severidad alta identificada como CVE-2022-20780 en la función de importación de Cisco Enterprise NFVIS podría permitir que un atacante remoto no autenticado filtre datos del sistema desde el host a cualquier máquina virtual configurada. Esta vulnerabilidad se debe a la resolución de entidades externas en el analizador XML. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un administrador para que importe un archivo manipulado que leerá datos del host y los escribirá en cualquier máquina virtual configurada. Una explotación exitosa podría permitir que el atacante acceda a la información del sistema desde el host, como archivos que contienen datos de usuario, en cualquier máquina virtual configurada.

  Cabe señalar que si un atacante que ya tiene acceso autenticado en una VM que está configurada dentro del host NFVIS podría obtener acceso directo a la información confidencial del sistema.
- Las vulnerabilidades no dependen unas de otras. No se requiere la explotación de una de las vulnerabilidades para explotar otra vulnerabilidad. Además, es posible que una versión de software que se vea afectada por una de las vulnerabilidades no se vea afectada por las otras vulnerabilidades.

3. Productos afectados:

- Estas vulnerabilidades afectan a Cisco Enterprise NFVIS anteriores a la versión 4.0 y 4.0, en la configuración predeterminada.

4. Solución:

Se recomienda actualizar Cisco Enterprise NFVIS a la versión 4.7.1 que aborda estas vulnerabilidades.

Fuentes de información	▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-NFVIS-MUL-7DySRX9

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 122	Fecha: 04-05-2022
		Página 6 de 8

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de falso servicio del correo electrónico de Microsoft.		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G02
Clasificación temática familia	Fraude		

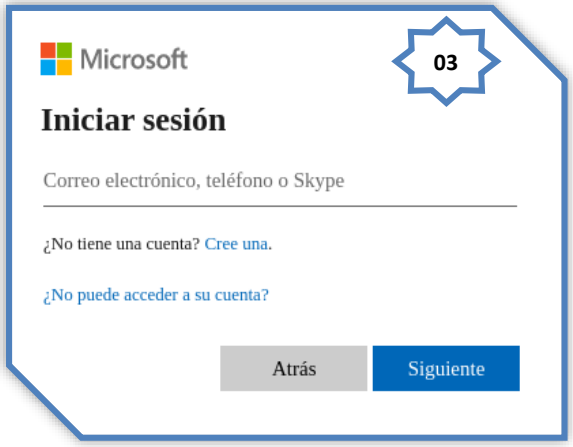
Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que los ciberdelincuentes vienen llevando a cabo una campaña de Phishing dirigidos a usuarios del servicio de correo electrónico proporcionados por Microsoft, por medio de la creación de un sitio web falso similar al oficial Microsoft Office, con el objetivo de robar credenciales de acceso de la cuenta del usuario.

2. Detalles del proceso de Phishing

Sitio web falso que suplanta la identidad de Microsoft Office, solicita a la víctima, iniciar sesión del usuario (correo electrónico, teléfono o Skype).

Una vez ingresado el usuario y hecho clic en <Próximo>, requiere ingresar la contraseña para continuar con el acceso.



Pasado unos segundos, es redirigido al sitio oficial de Microsoft, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados.

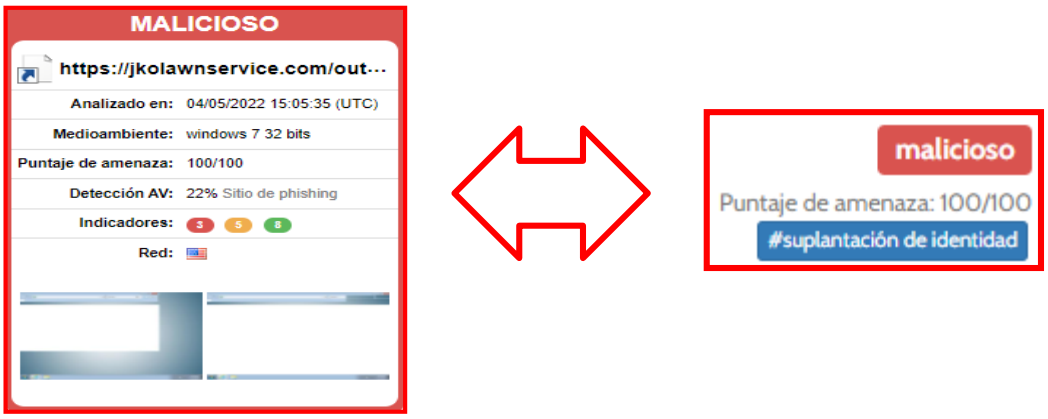
3. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que VEINTIUNO (21) proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD - PHISHING**.

alphaMountain.ai	Suplantación de identidad	Avira	Suplantación de identidad
BitDefender	Malware	Veredicto de Comodo Valkyrie	Suplantación de identidad
CRDF	Malicioso	CyRadar	Malicioso
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Malware	Navegación segura de Google	Suplantación de identidad
Seguridad Heimdal	Suplantación de identidad	kaspersky	Suplantación de identidad
Leonico	Suplantación de identidad	netcraft	Malicioso

4. INDICADORES DE COMPROMISO

- **URL** : hxxps://jkolawnservice[.]com/Outlook/index[.]html
- **SERVIDOR** : Apache
- **SHA-256** : 77f6fcf95298a710dcf84e702411593f49b47f7173e88536d702e760089a682a
- **IP** : 192[.]185[.]21[.]115
- **Dominio** : jkolawnservice.com

5. OTRAS DETENCIONES



6. Apreciación de la información:

- La presente campaña de Phishing, permite a los actores de amenazas obtener las credenciales de acceso del servicio del correo electrónico en la web de la compañía Microsoft (Outlook, Hotmail, etc.).

- El medio de propagación del sitio web fraudulento es a través de los correos electrónicos, donde ciberdelincuentes adjuntando enlaces de sitios web preparados con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger y mensajes de textos SMS.

7. Algunas Recomendaciones:

- Verificar detalladamente las URL de los sitios web
- No abrir o descargar archivos sospechosos.
- Mantener el antivirus actualizado.
- Descargar aplicaciones de fuentes confiables.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético