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

147-2024-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°147	Fecha: 25-06-2024
		Página: 4 de 11

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Acortador de URL en un archivo de Microsoft Word que conduce a Remcos RAT		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Recientemente, se encontró un documento de Word (FAKTURA.docx) que implementa el troyano de acceso remoto Remcos (RAT)

El malware RAT Remcos (Control remoto y vigilancia) proporciona a los atacantes un control total sobre un sistema infectado. Puede utilizarse para robo de datos, espionaje y otras actividades maliciosas. Comprender cómo se introduce normalmente este tipo de malware a través de archivos de Office puede ayudar a reconocer y mitigar estas amenazas.

2. DETALLES:

El ataque comienza con un correo electrónico que contiene un archivo adjunto .docx diseñado para engañar al destinatario.

Al examinar este archivo, se encuentra una URL acortada, lo que indica intenciones maliciosas. Esta URL redirecciona para descargar una variante del malware Equation Editor en formato RTF.

Al explotar la vulnerabilidad del Editor de ecuaciones (CVE-2017-11882), el malware, intenta descargar un script VB compuesto por una larga secuencia de variables y cadenas concatenadas, probablemente codificadas u ofuscadas. Estas cadenas forman una carga útil codificada, que puede decodificarse o ejecutarse más adelante en el script. El script VB se desofusca en un código PowerShell que intenta descargar un binario malicioso a través de una imagen esteganográfica y cadenas codificadas en Base64 inversas. Aunque se realiza una llamada de comando y control (C2), también hay una reconexión TCP, lo que sugiere que es posible que el C2 no esté disponible. El análisis de DNS pasivo identificó los dominios C2, pero actualmente están inactivos.

El documento (SHA1: f1d760423da2245150a931371af474dda519b6c9) contiene dos archivos críticos: settings.xml.rels y document.xml.rels ubicados en word/_rels/.

El archivo settings.xml.rels revela una URL abreviada responsable de descargar la siguiente etapa de la infección.

La ejecución del archivo .docx en un entorno sandbox revela que contiene la vulnerabilidad CVE-2017-0199.

Al explotar esta vulnerabilidad, el documento intenta conectarse a un servidor remoto para descargar un archivo malicioso.

El atacante utiliza un servicio de acortamiento de URL para enmascarar la URL maliciosa, lo que dificulta que la víctima reconozca el riesgo y ayuda a eludir los filtros de seguridad que podrían señalar URL sospechosas.

Una investigación más profunda de la carpeta \word\embeddings revela archivos PDF incrustados dentro de los archivos bin de oleObject.

El archivo PDF parece benigno y muestra una transacción bancaria entre una empresa y un banco. Sin embargo, la verdadera amenaza reside en el archivo RTF (SHA1: 539deaf1e61fb54fb998c54ca5791d2d4b83b58c) descargado a través de la URL abreviada.

Este archivo aprovecha la vulnerabilidad del Editor de ecuaciones para descargar un script VB (SHA1: 9740c008e7e7eef31644ebddf99452a014fc87b4).

El script parece ser una larga cadena de variables y cadenas concatenadas, datos potencialmente codificados u ofuscados. La variable importante es “remercear”, que se asigna a una cadena concatenada muy larga. Parece construirse concatenando repetidamente “maleta”, “centralizador” y varios literales de cadena. El uso de concatenación repetida sugiere que “remercear” se está construyendo para contener alguna información o comando codificado. La cadena concatenada representa una carga útil codificada, que podría decodificarse o ejecutarse en un punto posterior del script.

Después de la desofuscación, el código de PowerShell intenta descargar un binario malicioso desde dos URL diferentes. Primero, descarga el malware en el sistema utilizando el método de esteganografía, a través de una URL, es decir: hxxps://uploaddeimagens[.]com.br/images/004/785/720/original/new_image.jpg?1716307634.

La imagen contiene una larga cadena codificada en Base64, cuyos primeros seis bytes se decodifican en 'MZ', lo que indica la presencia de un ejecutable de Windows.

La imagen indica que se está produciendo un ataque a través del "grupo Deathnote", y el símbolo L sugiere que el grupo Lazarus está detrás de este ataque.

En segundo lugar, se comunica a una IP, es decir, 96.126.101[.]128 para obtener un archivo TXT, es decir, hxxp://96[.]126.101[.]128/43009/NGB.txt (como se muestra en PowerShell desofuscado en orden inverso). El archivo TXT contiene una cadena codificada en base 64 inversa.

Los atacantes crean un binario malicioso codificando primero en Base64 y luego invierten la cadena codificada en Base64 resultante. Esto añade una capa de ofuscación, ya que los datos codificados no parecen ser Base64 de inmediato y, por lo tanto, evaden mecanismos de detección simples. Con la ayuda de Cyber Chef, invertimos la cadena y luego realizamos el esquema de decodificación Base64 para generar una carga maliciosa, es decir, sha1: 83505673169efb06ab3b99d525ce51b126bd2009

La supervisión de los procesos revela una conexión a un servidor C2 potencial (IP: 94[.]156[.]66[.]67:2409), que actualmente está inactivo, lo que resulta en una reconexión TCP.

Indicadores de Compromiso:

Sujeto	FAKTURA
Remitentes de sobres	• info[arroba]cieloqistics[.com • info[arroba]pluse-tr[.com • export[arroba]aautomatotools[.store • info[arroba]tongunpano[.icu

FAKTURA.docx	f1d760423da2245150a931371af474dda519b6c9
URL	• hxxp://ilang.in/QNkGv • hxxp[://]96[.]126[.]101[.]128/43009/mnj/lionskingalwaysbeakingofjungletoentenderqué tan rápido regresa el rey de la jungla con todas las cosas para llevarme de regreso al juego___lionsarekingofjunglealways[.]doc
rtf	539sordo1e61fb54fb998c54ca5791d2d4b83b58c
URL de descarga de scripts de VB	hxxps[://]paste[.]ee/d/HdLtf
secuencia de comandos VB	9740c008e7e7eef31644ebddf99452a014fc87b4
Archivo TXT de cadenas codificadas en base64 inversa	hxxp[://]96[.]126[.]101[.]128/43009/NGB[.]txt
Archivo de imagen esteganográfica	hxxps://uploaddeimagens[.]com.br/images/004/785/720/original/new_image.jpg?1716307634
Remcos binario	83505673169efb06ab3b99d525ce51b126bd2009
IP C2	94.156.66[.]67:2409
Dominios C2	• newsat[.]duckdns[.]org • belgom[.]duckdns[.]org • fordede[.]duckdns[.]org • logili[.]duckdns[.]org

3. RECOMENDACIONES:

- Realizar el bloqueo de los indicadores de compromiso listados.
- Practicar una higiene estricta de contraseñas. Utilizar contraseñas únicas para cada aplicación como gestor de contenidos, servicio web, base de datos y cambiarlas periódicamente.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- 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.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones. Los usuarios solo deben tener acceso a los recursos y datos necesarios para sus funciones.
- Implementar herramientas y procesos para vigilar de manera constante posibles intrusiones o explotaciones de vulnerabilidades.
- Educar a los usuarios sobre las amenazas de troyanos y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://gbhackers.com/beware-of-shorten-urls/ • hxxps://www.forcepoint.com/blog/x-labs/url-shortener-microsoft-word-remcos-rat-trojan

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°147	Fecha: 25-06-2024
		Página: 7 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en Creo Elements / Direct License Server de PTC		
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:

Thomas Riedmaier de Siemens Energy ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo falta de autorización en el servidor de licencia directa "Creo Elements" de PTC. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios del sistema operativo.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-6071 de tipo falta de autorización, se debe a que el servidor de licencia directa Creo Elements de PTC, expone una interfaz web que pueden utilizar atacantes remotos no autenticados para ejecutar comandos arbitrarios del sistema operativo en el servidor.

A. Productos afectados:

Las siguientes versiones de Creo Elements / Direct License Server se ven afectadas; esta vulnerabilidad no afecta al "servidor de licencias Creo":

- Creo Elements / Direct License Server: versión 20.7.0.0 y anteriores.

3. RECOMENDACIÓN:

- Actualizar a Creo Elements / Direct License Server 20.7.0.1 o una versión superior que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-177-02

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°147	Fecha: 25-06-2024
		Página: 8 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de validación de entrada incorrecta en los servicios 800xA de ABB		
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:

Uri Sade, Roman Dvorkin, Ariel Harush y Eran Jacob de OTORIO, han reportado ABB una vulnerabilidad de severidad **MEDIA** de tipo validación de entrada incorrecta que afecta a los servicios 800xA en nodos cliente/servidor basados en PC. Los controladores no se ven afectados por esta vulnerabilidad. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante provocar que los servicios fallen y se reinicien.

2. DETALLES:

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-3036 de tipo validación de entrada incorrecta en los servicios 800xA en nodos cliente/servidor basados en PC, podría permitir a un atacante que aprovechara esta vulnerabilidad podría provocar que los servicios fallaran y se reiniciaran enviando mensajes específicamente diseñados.

A. Productos afectados:

- ABB 800xA Base: versiones 6.1.1-2 y anteriores.

3. RECOMENDACIÓN:

- Actualizar a una versión activa del producto para obtener las últimas correcciones. El problema se corrige o se corregirá en las siguientes versiones del producto:
  - ABB 800xA Base 6.2.0-0 (parte del Sistema 800xA 6.2.0.0).
  - ABB 800xA Base 6.1.1-3 (parte del Sistema 800xA 6.1.1.2).
  - ABB 800xA Base 6.0.3-x (incluido en la próxima revisión).

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-177-01

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°147	Fecha: 25-06-2024
		Página: 9 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de inyección LDAP en Dogtag PKI		
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 LDAP en Dogtag PKI. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto eludir el proceso de autenticación.

2. **DETALLES:**

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-4727 de tipo inyección LDAP, podría permitir a un atacante remoto eludir el proceso de autenticación. La vulnerabilidad existe debido a una validación de entrada incorrecta al procesar consultas DLAP. Un atacante remoto no autenticado puede pasar un parámetro de cadena de consulta sessionID=* y autenticarse con una sesión existente guardada en el servidor de directorio LDAP.

Una falla en dogtag-pki y pki-core, en el esquema de autenticación de token, se puede omitir con una inyección LDAP. Al pasar el parámetro de cadena de consulta sessionID=*, un atacante puede autenticarse con una sesión existente guardada en el servidor de directorio LDAP, lo que puede provocar una escalada de privilegios.

A. **Productos afectados:**

- PKI: 11.0.0 - 11.4.3.

3. **RECOMENDACIÓN:**

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

Fuente de Información:	• hxxp://bugzilla.redhat.com/show_bug.cgi?id=2232218 • hxxp://github.com/dogtagpki/pki/commit/54e5b3c5932ad634b5ddf5b1d4d88c9419d6f720 • hxxp://github.com/dogtagpki/pki/commit/aa7161ba378caf5cf0471aafb679a842679c8388

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°147	Fecha: 25-06-2024
		Página: 10 de 11

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el cliente Citrix Secure Access para Linux y Mac/iOS		
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 **CRÍTICA** de tipo autenticación faltante para función crítica y violación de límites de confianza en el cliente Citrix Secure Access para Linux y Mac/iOS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante en la misma red local que la víctima lea, interrumpa o modifique el tráfico de red que se espera esté protegido por la VPN.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-3661 de tipo autenticación faltante para función crítica y violación de límites de confianza en el cliente Citrix Secure Access para Linux y Mac/iOS, se debe a que el protocolo de configuración dinámica de host (DHCP) puede agregar rutas a la tabla de enrutamiento de un cliente mediante la opción de ruta estática sin clases (121). Las soluciones de seguridad basadas en VPN que dependen de rutas para redirigir el tráfico pueden verse obligadas a filtrar tráfico a través de la interfaz física. Un atacante en la misma red local puede leer, interrumpir o posiblemente modificar el tráfico de red que se esperaba que estuviera protegido por la VPN.

La vulnerabilidad afecta a ciertas soluciones de seguridad basadas en VPN, incluida la aplicación GlobalProtect en sistemas Windows (no afectado), macOS y Linux, así como FortiClient en varias plataformas. Android no se ve afectado ya que no implementa soporte para la opción DHCP 121. El problema surge de la forma en que estos clientes VPN manejan la opción DHCP 121, que puede ser manipulada por un atacante para redirigir el tráfico fuera del túnel VPN. Sin embargo, este ataque no permite al atacante descifrar HTTPS u otro tráfico cifrado.

A. Productos afectados:

- Cliente Citrix Secure Access para Linux todas las versiones.
- Cliente Citrix Secure Access para versiones Mac e iOS anteriores a la 24.06.1.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad.
- Mitigar esta vulnerabilidad de acuerdo con las siguientes recomendaciones que indicó Citrix:
  - Para el cliente Citrix Secure Access para Linux, en una próxima versión se publicará una solución que solucione este problema.
  - Para el cliente Citrix Secure Access para Mac/iOS, los clientes que usan MDM deben configurar 'EnforceRoutes' en '1' en la configuración de VPN administrada y establecer el acceso a la LAN local en 'OFF' en la puerta de enlace. Los clientes que no utilicen MDM deben instalar la última actualización (24.06.1) y configurar los mismos ajustes.
- Implementar DHCP snooping, protecciones ARP y seguridad de puertos en los conmutadores para ayudar a prevenir servidores DHCP no autorizados en la red. También pueden obviar la opción 121 de DHCP cuando se utiliza una VPN, aunque esto podría causar problemas de conectividad en algunos escenarios.

Fuente de Información:	• hxxps://support.citrix.com/article/CTX677069/cloud-software-group-security-advisory-for-cve20243661 • hxxps://www.cve.org/CVERecord?id=CVE-2024-3661

Índice alfabético