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, 03 de Mayo de 2022

N° 121-2022-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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 121	Fecha: 03-05-2022
		Página 3 de 7

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidades en conmutadores de red Aruba y Avaya: TLStorm 2.0		
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

I. DATOS GENERALES:

CVE-2022-23676: Ejecución remota de código

Investigadores: Firma de seguridad de IoT Armis.

Los investigadores de seguridad cibernética han detallado hasta cinco fallas de seguridad graves en la implementación del protocolo TLS en varios modelos de conmutadores de red de Aruba y Avaya que podrían utilizarse para obtener acceso remoto a redes empresariales y robar información valiosa.

II. EVIDENCIA:

- Según el investigador, señaló que las fallas de diseño se remontan a una fuente común: un mal uso de NanoSSL, una suite de desarrollo SSL basada en estándares de Mocana, una subsidiaria de DigiCert.
- El nuevo conjunto de fallas, denominado TLStorm 2.0, hace que los conmutadores de red de Aruba y Avaya presenten vulnerabilidades.
- Los dispositivos afectados incluyen Avaya ERS3500 Series, ERS3600 Series, ERS4900 Series y ERS5900 Series, así como Aruba 5400R Series, 3810 Series, 2920 Series, 2930F Series, 2930M Series, 2530 Series y 2540 Series.
- La ejecución remota de código, permite que un adversario controle los dispositivos, se mueva lateralmente a través de la red y exfiltre datos confidenciales.

III. TEMA:

- Los hallazgos siguen a la divulgación de marzo de TLStorm, un conjunto de tres fallas críticas en los dispositivos APC Smart-UPS que podrían permitir que un atacante tome el control y, peor aún, dañe físicamente los dispositivos.
- La falta de cumplimiento de las pautas relacionadas con la biblioteca NanoSSL podría resultar en la ejecución remota de código.

La lista de errores de ejecución remota de código es la siguiente:

- CVE-2022-23676 (puntuación CVSS: 9,1): dos vulnerabilidades de corrupción de memoria en la implementación del cliente RADIUS de los conmutadores Aruba
- CVE-2022-23677 (puntuación CVSS: 9,0): uso indebido de NanoSSL en múltiples interfaces en conmutadores Aruba
- CVE-2022-29860 (puntuación CVSS: 9,8): vulnerabilidad de desbordamiento del montón de reensamblaje de TLS en los conmutadores de Avaya
- CVE-2022-29861 (puntaje CVSS: 9.8): vulnerabilidad de desbordamiento de pila de análisis de encabezado HTTP en conmutadores de Avaya
- Vulnerabilidad de desbordamiento de montón en el manejo de solicitudes HTTP POST en una línea de productos Avaya descontinuada (sin CVE).

IV. CONCLUSIÓN:

- "Estos resultados de la investigación son significativos, ya que destacan que la infraestructura de la red en sí está en riesgo y es explotable por los atacantes, lo que significa que la segmentación de la red por sí sola ya no es suficiente como medida de seguridad", dijo Barak Hadad, jefe de investigación en ingeniería de Armis.

V. RECOMENDACIÓN:

- Se recomienda encarecidamente a las organizaciones, que implementen dispositivos Avaya y Aruba afectados, que apliquen los parches para mitigar cualquier posible intento de explotación.

Fuentes de información	▪ hxxps://www.enhacke.com/2022/05/los-errores-criticos-de-tlstorm-2-0-afectan-a-los-conmutadores-de-red-aruba-y-avaya-ampliamente-utilizados/ ▪ hxxps://www.armis.com/blog/tlstorm-2-nanossl-tls-library-misuse-leads-to-vulnerabilities-in-common-switches/ ▪ hxxps://www.mocana.com/hubfs/pages-resources/datasheets/datasheet-Mocana-NanoSSL.pdf

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 121**	**Fecha: 03-05-2022**
		Página 5 de 7

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en el software Adaptive Security Appliance y Firepower Threat Defense de Cisco		
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 una vulnerabilidad de severidad ALTA de tipo asignación de privilegios incorrecta que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado elevar privilegios al nivel 15 en la interfaz de administración web del dispositivo afectado.

2. Detalles:

- La vulnerabilidad de asignación de privilegios incorrecta, se debe a que un producto asigna incorrectamente un privilegio a un actor en particular, creando una esfera de control no deseada para ese actor.
- La vulnerabilidad identificada como CVE-2022-20759 en la interfaz de servicios web para las funciones VPN de acceso remoto del software Cisco Adaptive Security Appliance (ASA) y el software Cisco Firepower Threat Defense (FTD) podría permitir que un atacante remoto autenticado, pero sin privilegios, eleve los privilegios al nivel 15.
- Esta vulnerabilidad se debe a la separación incorrecta de los ámbitos de autenticación y autorización. Un atacante podría explotar esta vulnerabilidad enviando mensajes HTTPS manipulados a la interfaz de servicios web de un dispositivo afectado. Una explotación exitosa podría permitir que el atacante obtenga acceso de nivel de privilegio 15 a la interfaz de administración web del dispositivo. Esto incluye acceso de nivel de privilegio 15 al dispositivo mediante herramientas de administración como Cisco Adaptive Security Device Manager (ASDM) o Cisco Security Manager (CSM).

3. Productos afectados:

- Software Cisco ASA, versión 9.7 y anteriores, 9.8, 9.9, 9.10, 9.12, 9.13, 9.14, 9.15, 9.16 y 9.17;
- Software Cisco FTD, versión 6.2.2 y anteriores, 6.2.3, 6.3.0, 6.4.0, 6.5.0, 6.6.0, 6.7.0, 7.0.0 y 7.1.0.

Esta vulnerabilidad afecta a los productos de Cisco si ejecutan una versión vulnerable del software Cisco ASA o del software Cisco FTD y al menos una de las siguientes condiciones es verdadera:

- HTTPS Management Access y IKEv2 Client Services están habilitados en al menos una (no necesariamente la misma) interfaz;
- HTTPS Management Access y WebVPN están habilitados en al menos una (no necesariamente la misma) interfaz.

Ninguna de estas funciones está habilitada de manera predeterminada en el software Cisco ASA o el software Cisco FTD.

4. Solución:

- Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. Las versiones 6.2.2 y anteriores del software FMC y FTD de Cisco, así como las versiones 6.3.0 y 6.5.0, han llegado al final del mantenimiento del software.

Fuentes de información	▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-mgmt-privesc-BMFMUvye

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 121	Fecha: 03-05-2022
		Página 6 de 7

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en Kaspersky Anti-Virus y Endpoint Security		
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:

Kaspersky ha reportado una vulnerabilidad de severidad MEDIA de tipo inyección de código en Kaspersky Anti-Virus y Endpoint Security. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado ejecutar código arbitrario en el sistema de destino.

2. Detalles:

- La vulnerabilidad de inyección de código se debe a que el software construye todo o parte de un segmento de código utilizando la entrada influenciada externamente desde un componente ascendente, pero no neutraliza o neutraliza incorrectamente elementos especiales que podrían modificar la sintaxis o el comportamiento del segmento de código previsto.
- La vulnerabilidad identificada como CVE-2022-27534 de inyección de código podría permitir a un atacante remoto ejecute código arbitrario en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada incorrecta en un módulo de análisis de datos. Un usuario remoto puede enviar una solicitud especialmente diseñada y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso completo del sistema vulnerable.

3. Productos afectados:

- Kaspersky Anti-Virus: anteriores a la versión 12.03.2022;
- Kaspersky Internet Security: anteriores a la versión 12.03.2022;
- Total, Security: anteriores a la versión 12.03.2022;
- Small Office Security: anteriores a la versión 12.03.2022;
- Security Cloud: anteriores a la versión 12.03.2022;
- Endpoint Security: anteriores a la versión 12.03.2022.

4. Solución:

- Kaspersky recomienda actualizar los productos afectados a la última versión disponible que corrige esta vulnerabilidad.

Fuentes de información	▪ hxxps://support.kaspersky.com/general/vulnerability.aspx?el=12430#310322_2 ▪ hxxps://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27534

Índice alfabético