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

246-2024-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°246	Fecha: 24-10-2024 Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Una base de datos de la ONU quedó expuesta y dejó información sensible en línea		
Tipo de Ataque	Fuga de Información		FugaInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K02
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

El investigador de ciberseguridad Jeremiah Fowler descubrió una base de datos mal configurada que afectaba al Fondo Fiduciario de las Naciones Unidas (ONU) para eliminar la Violencia contra la Mujer. Según la investigación, la base de datos expuesta no estaba protegida por una contraseña o cualquier otro método de autenticación de seguridad, lo que la hacía fácilmente accesible para cualquier persona con una conexión a Internet.

2. DETALLES:

La base de datos contenía más de 115.000 registros y 228 GB de datos confidenciales, incluidos informes financieros, documentos del personal, direcciones de correo electrónico, contratos e información personal de víctimas y trabajadores de organizaciones benéficas en formatos PDF, .XML, .JPG y PNG.

Los documentos filtrados revelaron una amplia gama de información confidencial, como:

- Información del personal: nombres, datos fiscales, información salarial y funciones laborales.
- Información de las víctimas: nombres, direcciones de correo electrónico y experiencias personales.
- Detalles financieros: Información de cuentas bancarias, auditorías e informes financieros.
- Documentos organizativos: Contratos, certificaciones y documentos de registro.

Los registros indicaban una conexión con ONU Mujeres y el Fondo Fiduciario de las Naciones Unidas para eliminar la violencia contra la mujer, con cartas de referencia, logotipos de las Naciones Unidas y nombres de archivos que indicaban su asociación.

Los datos expuestos podrían ser utilizados por agentes maliciosos para atacar a personas y organizaciones asociadas con el Fondo Fiduciario de las Naciones Unidas.

Por ejemplo, los delincuentes pueden lanzar ataques de phishing selectivos, robo de identidad, intentos de chantaje, fraude, extorsión y acoso.

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos o no solicitados. En su lugar, visitar el sitio web escribiendo la dirección directamente en su navegador.
- Monitorear los movimientos de su cuenta bancaria afectada con el fin de detectar cargos no autorizados e informarlos a su entidad.
- Tener cuidado con las estafas telefónicas que podrían implicar la explotación de los datos robados.
- Practicar una higiene estricta de contraseñas. Utilizar contraseñas únicas para cada tarjeta y cambiarlas periódicamente.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Implementar medidas rigurosas de evaluación y monitoreo de proveedores, cifrado de datos regular, protocolos de autenticación de usuarios, para salvar sus datos y la confianza de sus clientes.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://es.wired.com/articulos/una-base-de-datos-de-la-onu-quedo-expuesta-y-dejo-informacion-sensible-en-linea • hxxps://hackread.com/misconfigured-un-database-gender-violence-victims-data/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°246	Fecha: 24-10-2024
		Página: 5 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades de severidad crítica en productos Cisco		
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 publicado múltiples vulnerabilidades de severidad **CRÍTICA** de tipo uso de contraseñas codificadas, Inyección de comando del SO y neutralización incorrecta de delimitadores de expresiones y comandos que afectan a productos Cisco. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante local no autenticado acceder a un sistema afectado utilizando credenciales estáticas, asimismo un atacante remoto autenticado podría ejecutar comandos arbitrarios en el sistema operativo subyacente como root.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-20412 de tipo uso de contraseñas codificadas en el software Cisco Firepower Threat Defense (FTD) para Cisco Firepower Series 1000, 2100, 3100 y 4200, podría permitir que un atacante local no autenticado acceda a un sistema afectado utilizando credenciales estáticas. Esta vulnerabilidad se debe a la presencia de cuentas estáticas con contraseñas codificadas en el sistema afectado. Un atacante podría aprovechar esta vulnerabilidad iniciando sesión en la CLI de un dispositivo afectado con estas credenciales. Una explotación exitosa podría permitir al atacante acceder al sistema afectado y recuperar información confidencial, realizar acciones limitadas de resolución de problemas, modificar algunas opciones de configuración o hacer que el dispositivo no pueda iniciarse en el sistema operativo, lo que requeriría una nueva imagen del dispositivo.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-20424 de tipo inyección de comando del SO en la interfaz de administración basada en web del software Cisco Secure Firewall Management Center (FMC), anteriormente Firepower Management Center Software, podría permitir que un atacante remoto autenticado ejecute comandos arbitrarios en el sistema operativo subyacente como root. Esta vulnerabilidad se debe a una validación de entrada insuficiente de ciertas solicitudes HTTP. Un atacante podría aprovechar esta vulnerabilidad autenticándose en la interfaz de administración basada en web de un dispositivo afectado y luego enviando una solicitud HTTP diseñada al dispositivo. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios con permisos de root en el sistema operativo subyacente del dispositivo Cisco FMC o ejecutar comandos en dispositivos Cisco FTD administrados. Para aprovechar esta vulnerabilidad, el atacante necesitaría credenciales válidas para una cuenta de usuario con al menos el rol de Analista de seguridad (solo lectura).

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-20329 de tipo neutralización incorrecta de delimitadores de expresiones y comandos en el subsistema SSH del software Cisco Adaptive Security Appliance (ASA), podría permitir que un atacante remoto autenticado ejecute comandos del sistema operativo como root. Esta vulnerabilidad se debe a una validación insuficiente de la entrada del usuario. Un atacante podría aprovechar esta vulnerabilidad enviando una entrada manipulada al ejecutar comandos CLI remotos a través de SSH. Una explotación exitosa podría permitir al atacante ejecutar comandos en el sistema operativo subyacente con privilegios de nivel raíz. Un atacante con privilegios de usuario limitados podría usar esta vulnerabilidad para obtener control total sobre el sistema.

Para las vulnerabilidades de severidad **alta** se han asignado los siguientes identificadores: CVE-2024-20420, CVE-2024-20421, CVE-2024-20458, CVE-2024-20459, CVE-2024-20460, CVE-2024-20461, CVE-2024-20462, CVE-2024-20463CVE-2024-20351, CVE-2024-20330, CVE-2024-20339, CVE-2024-20260, CVE-2024-20402, CVE-2024-20268, CVE-2024-20485, CVE-2024-20426, CVE-2024-20408, CVE-2024-20495, CVE-2024-20494, CVE-2023-20063.

Para las vulnerabilidades de severidad **media** se han asignado los siguientes identificadores: CVE-2024-20377, CVE-2024-20387, CVE-2024-20388, CVE-2024-20342, CVE-2024-20407, CVE-2024-20431, CVE-2024-20264, CVE-2024-20269, CVE-2024-20273, CVE-2024-20298, CVE-2024-20300, CVE-2024-20364, CVE-2024-20372, CVE-2024-20386, CVE-2024-20403, CVE-2024-20409, CVE-2024-20410, CVE-2024-20415, CVE-2024-20340, CVE-2024-20471, CVE-2024-20472, CVE-2024-20473, CVE-2024-20482, CVE-2024-20274, CVE-2024-20379, CVE-2024-20275, CVE-2024-20374, CVE-2024-20474, CVE-2024-20341, CVE-2024-20382, CVE-2024-20384, CVE-2024-20481, CVE-2024-20297, CVE-2024-20331, CVE-2024-20299, CVE-2024-20493, CVE-2024-20526, CVE-2024-20370.

A. Productos afectados:

- La vulnerabilidad CVE-2024-20412 afecta a los siguientes productos de Cisco si ejecutan el software Cisco FTD versión 7.1 a 7.4 con una versión de base de datos de vulnerabilidades (VDB) 387 o anterior: Firepower Series 1000, 2100, 3100 y 4200;
- La vulnerabilidad CVE-2024-20424 afecta a los productos Cisco si ejecutan una versión vulnerable del software Cisco FMC, independientemente de la configuración del dispositivo;
- La vulnerabilidad CVE-2024-20329 afecta a los productos Cisco si ejecutan una versión vulnerable del software Cisco ASA y tienen la pila CiscoSSH habilitada y el acceso SSH permitido en al menos una interfaz.

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-ftd-statcred-dFC8tXT5 • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-v3AWDqN7 • hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssh-rce-gRAuPEUF

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°246	Fecha: 24-10-2024
		Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en dispositivos de servicio en la nube de Ivanti (CSA)		
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 publicado una vulnerabilidad de severidad **CRÍTICA** de tipo recorrido de ruta (Path Traversal) que afecta a Ivanti Cloud Service Appliance (CSA). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado acceder a funciones restringidas en los sistemas afectados.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-8963 de tipo recorrido de ruta en Ivanti Cloud Service Appliance, podría permitir a un atacante remoto no autenticado acceder a funciones restringidas dentro del dispositivo. Un atacante puede explotar esta vulnerabilidad sin ninguna interacción del usuario, puede ejecutarse a través de una red.

La vulnerabilidad se ha incluido en el Catálogo de vulnerabilidades explotadas conocidas de la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA), lo que destaca su explotación activa en la naturaleza. Si la vulnerabilidad CVE-2024-8963 se usa junto con CVE-2024-8190, que es un fallo de inyección de comandos del sistema operativo, un atacante puede eludir la autenticación de administrador y ejecutar comandos arbitrarios en el dispositivo.

A. Productos afectados:

- Ivanti Cloud Service Appliance, versiones anteriores a la 4.6 Patch 519, incluidos parches anteriores como 512 y 518.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 5.0 que aborda esta vulnerabilidad. Ivanti CSA 4.6 está en el final de su vida útil y ya no recibe parches para SO o bibliotecas de terceros. Además, con el estado de fin de vida útil, la corrección publicada el 10 de septiembre es la última corrección que Ivanti implementará en esa versión. Los clientes deben actualizar a Ivanti CSA 5.0 para recibir soporte continuo. CSA 5.0 es la única versión compatible del producto y no se ve afectada por esta vulnerabilidad.

Fuente de Información:	• hxxps://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/critical-vulnerability-ivanti-csa-46-cloud-services-appliance • hxxps://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963 • hxxps://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963?language=en_US

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°246	Fecha: 24-10-2024 Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en dispositivos de comunicaciones Ethernet DSE855 de Deep Sea Electronics		
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 publicado una vulnerabilidad de severidad **ALTA** de tipo falta de autenticación para una función crítica que afecta a los dispositivos de comunicaciones Ethernet DSE855 de Deep Sea Electronics. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante acceder a las credenciales almacenadas y divulgar información confidencial sobre las instalaciones afectadas.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-5947 de tipo falta de autenticación para una función crítica que afecta a los dispositivos de comunicaciones Ethernet DSE855, podría permitir a un atacante acceder a las credenciales almacenadas y divulgar información confidencial sobre las instalaciones afectadas. No se requiere autenticación para explotar esta vulnerabilidad. La vulnerabilidad existe dentro de la interfaz de usuario basada en web. El problema es el resultado de la falta de autenticación antes de permitir el acceso a la funcionalidad.

DSE855 de Deep Sea Electronics es vulnerable a una divulgación de configuración cuando se hace referencia directa al objeto Backup.bin mediante una solicitud HTTP GET.

A. Productos afectados:

- DSE855: Versión 1.0.26.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 1.2.0 o posterior para mitigar esta vulnerabilidad.
- Minimizar la exposición de la red para los sistemas de control.
- Aislar las redes del sistema de control de las redes comerciales.
- Utilizar métodos de acceso remoto seguros como VPN.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-298-03 • hxxps://www.cve.org/CVERecord?id=CVE-2024-5947

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°246	Fecha: 24-10-2024 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en productos de Microsoft		
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:

Microsoft Corporation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo condición de carrera de tiempo de uso y verificación de tiempo (TOCTOU) que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución remota de código arbitrario.

2. DETALLES:

CBL-Mariner es una distribución de Linux desarrollada por Microsoft, lanzada inicialmente en 2020. Su nombre, CBL, significa "Common Base Linux". Esta distribución está diseñada específicamente para servir como el sistema operativo base para contenedores en la infraestructura de Microsoft Azure, incluyendo su uso en Azure Kubernetes Service (AKS) y Azure IoT Edge.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-0132 de tipo condición de carrera de tiempo de uso y verificación de tiempo que afecta a CBL Mariner 2.0 x64 y CBL Mariner 2.0 ARM, podría permitir a un atacante remoto no autenticado la ejecución remota de código arbitrario.

Los clientes con grupos de nodos de Azure Kubernetes Service (AKS) basados en Ubuntu Linux o Azure Linux que utilizan configuraciones de controlador de GPU NVIDIA se ven afectados por esta vulnerabilidad.

A. Productos afectados:

- Versiones ARM de CBL Mariner 2.0 anteriores a 1.16.2-1.
- Versiones CBL Mariner 2.0 x64 anteriores a 1.16.2-1.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0132 • hxxps://www.cve.org/CVERecord?id=CVE-2024-0132

Índice alfabético