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

089-2025-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°089	Fecha: 14-04-2025
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Fortinet advierte que atacantes pueden conservar el acceso después de la aplicación de parches		
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:**

A principios de la semana pasada, Fortinet comenzó a enviar correos electrónicos a sus clientes advirtiéndoles que sus dispositivos FortiGate/FortiOS estaban comprometidos según la telemetría recibida de los dispositivos FortiGuard.

Estos correos electrónicos se titulaban "Notificación de compromiso del dispositivo - FortiGate / FortiOS - ** Acción urgente requerida **", y se les daba una designación TLP:AMBER+STRICT.

2. **DETALLES:**

Fortinet advierte que los actores de amenazas utilizan una técnica de postexplotación que les ayuda a mantener acceso de solo lectura a dispositivos VPN FortiGate previamente comprometidos, incluso después de que se haya parcheado el vector de ataque original.

Fortinet publicó un aviso el jueves advirtiendo sobre esta nueva técnica de explotación.

El aviso indica que, cuando los actores de amenazas vulneraron servidores utilizando vulnerabilidades antiguas, crearon enlaces simbólicos en la carpeta de archivos de idioma al sistema de archivos raíz de los dispositivos con SSL-VPN habilitado.

Esto les permite mantener acceso de sólo lectura al sistema de archivos raíz a través del panel web SSL-VPN de acceso público incluso después de ser descubiertos y expulsados.

Se cree que los atacantes aprovecharon vulnerabilidades de seguridad conocidas y ahora parcheadas, incluyendo, entre otras, CVE-2022-42475, CVE-2023-27997, y CVE-2024-21762.

Fortinet afirmó que las modificaciones se realizaron en el sistema de archivos del usuario y lograron evadir la detección, lo que provocó que el enlace simbólico (también conocido como symlink) permaneciera incluso después de que se solucionaran las vulnerabilidades de seguridad responsables del acceso inicial.

Esto, a su vez, permitió a los actores de amenazas mantener acceso de solo lectura a los archivos del sistema de archivos del dispositivo, incluidas las configuraciones. Sin embargo, los clientes que nunca han habilitado SSL-VPN no se ven afectados por el problema.

3. **RECOMENDACIONES:**

- Actualizar sus instancias a las versiones 7.6.2, 7.4.7, 7.2.11, 7.0.17 o 6.4.16 de FortiOS.
- Revisar las configuraciones de los dispositivos que se consideren potencialmente comprometidas y realizar las acciones de recuperación adecuadas.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2025/04/fortinet-advierte-que-atacantes.html • hxxps://www.bleepingcomputer.com/news/security/fortinet-hackers-retain-access-to-patched-fortigate-vpns-using-symlinks/ • hxxps://hackread.com/fortinet-fixe-attackers-bypass-patches-maintain-access/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°089	Fecha: 14-04-2025 Página: 5 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en dispositivos D-Link DI-8100		
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:

La empresa D-Link Corporation ha publicado una vulnerabilidad de severidad **ALTA** de tipo restricción incorrecta de operaciones dentro de los límites de un búfer de memoria y desbordamiento de búfer basado en pila que afecta a dispositivos D-Link de la serie DI-8100. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante la ejecución de código arbitrario, comprometer la integridad del sistema y obtener acceso no autorizado en el dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-3538 de tipo desbordamiento de búfer en la pila en el dispositivo D-Link de la serie DI-8100, afecta a la función auth_asp del archivo /auth.asp del componente jhttpd. El ataque debe abordarse dentro de la red local. Esta vulnerabilidad puede explotarse manipulando el argumento 'callback'. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución de código arbitrario, comprometer la integridad del sistema y obtener acceso no autorizado en el dispositivo afectado.

Cabe indicar que existen pruebas de concepto (PoC) disponibles que explotan esta vulnerabilidad de manera activa.

A. Productos afectados:

- D-Link DI-8100, versión firmware 16.07.26A1.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de firmware disponible que abordan esta vulnerabilidad.
- Aislar los dispositivos D-Link DI-8100 afectados de las redes no confiables. Esto reduce el riesgo de explotación desde redes no autorizadas.
- Utilizar un firewall y configurado correctamente para bloquear el tráfico no deseado.
- Cambiar las contraseñas predeterminadas del router y asegúrate de que sean robustas.
- Habilitar la autenticación de dos factores (2FA) para agregar una capa adicional de seguridad.
- Desactivar las interfaces de administración remota.
- Implementar una segmentación estricta de la red.
- Monitorear el tráfico de la red para detectar actividades sospechosas.
- Reemplazar los dispositivos vulnerables o esperar un parche oficial del proveedor.
- Realizar una auditoría de seguridad completa en la red para identificar y mitigar otras posibles vulnerabilidades.
- Utilizar sistemas de detección/prevención de intrusiones de red para detectar posibles intentos de explotación.

Fuente de Información:	• hxxps://github.com/Fizz-L/CVE1/blob/main/DI-8100Command%20execution2.md • hxxps://vuldb.com/?ctiid.304577 • hxxps://vuldb.com/?id.304577 • hxxps://vuldb.com/?submit.524224 • hxxps://www.dlink.com/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°089	Fecha: 14-04-2025 Página: 6 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Microsoft Visual Studio Code		
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 **MEDIA** de tipo control de acceso inadecuado en Visual Studio Code (VS Code). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante provocar una escalada de privilegios localmente, lo que conduce a un acceso no autorizado a recursos confidenciales.

2. DETALLES:

Visual Studio Code (VS Code) es un entorno de desarrollo integrado (IDE) ligero, versátil y ampliamente utilizado, desarrollado por Microsoft.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-32726 de tipo control de acceso inadecuado en Microsoft Visual Studio Code, podría permitir a un atacante provocar una escalada de privilegios localmente.

Un atacante que aproveche con éxito esta vulnerabilidad podría ejecutar código en el contexto de otro usuario de Visual Studio Code en el sistema vulnerable. Un atacante que aproveche con éxito esta vulnerabilidad podría ver información confidencial (Confidencialidad) y modificar el código en el repositorio (Integridad), y podría interferir con la disponibilidad del código (Disponibilidad).

El control de acceso inadecuado en Visual Studio Code permite que un atacante autorizado eleve privilegios localmente.

A. Productos afectados:

- Microsoft Visual Studio Code, versiones anteriores a 1.99.1.

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-2025-32726

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°089	Fecha: 14-04-2025
		Página: 7 de 10

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

Palo Alto Networks Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo comprobación inadecuada de condiciones inusuales o excepcionales que afecta a la función de autenticación del Protocolo Simple de Inscripción de Certificados (SCEP) del software PAN-OS de Palo Alto Networks. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante no autenticado enviar un paquete especialmente diseñado que puede provocar que el firewall se reinicie repetidamente.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-0128 de tipo comprobación inadecuada de condiciones inusuales o excepcionales, podría permitir a un atacante no autenticado enviar un paquete especialmente diseñado que puede provocar que el firewall se reinicie repetidamente, lo que finalmente lo obliga a entrar en modo de mantenimiento e interrumpir el servicio.

La vulnerabilidad existe debido a una gestión incorrecta de errores en la función de autenticación del Protocolo Simple de Inscripción de Certificados (SCEP). Un atacante remoto puede enviar datos especialmente diseñados a la aplicación y realizar un ataque de denegación de servicio (DoS).

A. Productos afectados:

- Palo Alto PAN-OS: 10.1.0 anterior a 10.1.14.
- Palo Alto PAN-OS: 10.2.0-h1 anterior a 10.2.10.
- Palo Alto PAN-OS: 11.0.0-h1 anterior a 11.0.5.
- Palo Alto PAN-OS: 11.1.0-h1 anterior a 11.1.4.
- Palo Alto PAN-OS: 11.2.0 anterior a 11.2.2.
- Acceso Prisma: antes de 10.2.4-h36.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//security[.]paloaltonetworks[.]com/CVE-2025-0128

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°089	Fecha: 14-04-2025 Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Apache		
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:

Apache Software Foundation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo deserialización de datos no confiables que afecta a múltiples versiones de Apache Tomcat. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar comandos arbitrarios y comprometer el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-24813 de tipo deserialización de datos no confiables, podría permitir a un atacante cargar archivos de sesión serializados maliciosos en directorios grabables, que podría aprovecharse en un ataque de deserialización por el servidor, lo que provoca la ejecución de código arbitrario.

La vulnerabilidad existe debido a una validación insuficiente de la información proporcionada por el usuario al gestionar la carga de archivos mediante solicitudes HTTP PUT. Un atacante remoto puede enviar una solicitud HTTP PUT especialmente diseñada al servidor y obtener acceso a información confidencial o incluso ejecutar código arbitrario.

A. Productos afectados:

- Apache Tomcat: 9.0.0-M1 anterior a 9.0.98.
- Apache Tomcat: 10.0.0-M1 anterior a 10.0.27.
- Apache Tomcat: 10.1.0-M1 anterior a 10.1.34.
- Apache Tomcat: 11.0.0-M1 anterior a 11.0.2.

3. RECOMENDACIÓN:

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

Fuente de Información:	• https://www.openwall.com/lists/oss-security/2025/03/10/5 • https://www.vicarius.io/vsociety/posts/cve-2025-24813-detect-apache-tomcat-rce • https://www.vicarius.io/vsociety/posts/cve-2025-24813-mitigate-apache-tomcat-rce • https://security.netapp.com/advisory/ntap-20250321-0001/ • https://lists.debian.org/debian-lts-announce/2025/04/msg00003.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°089	Fecha: 14-04-2025 Página: 9 de 10

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

Rockwell Automation ha publicado una vulnerabilidad de severidad **ALTA** de tipo uso de variable no inicializada que afecta a Rockwell Automation Arena. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

Rockwell Automation Arena es un software de simulación utilizado principalmente para la simulación de eventos discretos, con capacidades adicionales de modelado de flujo y basado en agentes. Está diseñado para ayudar a las empresas a optimizar sus procesos mediante la creación de gemelos digitales de sus sistemas a partir de datos históricos. Esto permite a las empresas analizar y predecir el rendimiento del sistema, reducir riesgos y optimizar la toma de decisiones.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-2287 de uso de variable no inicializada, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

Esta vulnerabilidad existe debido a un puntero no inicializado, resultado de una validación incorrecta de los datos proporcionados por el usuario. Para explotar esta vulnerabilidad, un usuario legítimo debe abrir un archivo DOE (Diseño de Experimentos) malicioso. Si se explota con éxito, un atacante puede divulgar información confidencial y ejecutar código arbitrario en el sistema.

A. Productos afectados:

- Rockwell Automation Arena, versiones anteriores a: 16.20.08.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//www[.]rockwellautomation[.]com/en-us/trust-center/security-advisories/advisory.SD1726.html

Índice alfabético