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

026-2025-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°026	Fecha: 31-01-2025
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La vulnerabilidad de TeamViewer conduce a una escalada de privilegios		
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:

TeamViewer, la compañía del software de acceso remoto ampliamente utilizado, reveló el 28 de enero de 2025 que presenta una falla de seguridad que podría permitir a atacantes locales escalar privilegios.

2. DETALLES:

A la vulnerabilidad identificada como CVE-2025-0065 se le ha asignado una calificación de 7,8 en el Sistema de puntuación de vulnerabilidades común (CVSS), lo que la coloca en el rango de gravedad “Alta”.

La vulnerabilidad reside en el componente TeamViewer_service.exe de TeamViewer Full Client y Host en sistemas Windows.

Un atacante con acceso local sin privilegios a un sistema Windows podría aprovechar esta falla inyectando argumentos maliciosos en el componente vulnerable, aumentando así sus privilegios.

Si bien esta vulnerabilidad no permite la explotación remota, representa un riesgo significativo en entornos compartidos o multiusuario, como redes corporativas o sistemas de acceso público.

Afortunadamente, TeamViewer confirmó que, hasta la fecha, no hay evidencia de que esta vulnerabilidad haya sido explotada.

TeamViewer ha lanzado la versión 15.62 para solucionar este problema.

Productos afectados:

- Cliente completo de TeamViewer (Windows) : versiones anteriores a 15.62, 14.7.48799, 13.2.36226, 12.0.259319 y 11.0.259318.
- TeamViewer Host (Windows) : versiones anteriores a 15.62, 14.7.48799, 13.2.36226, 12.0.259319 y 11.0.259318.

3. RECOMENDACIONES:

- Actualizar su software a la última versión disponible 15.62. Las versiones actualizadas se pueden descargar desde el sitio web oficial de TeamViewer.
- Mantenerse informados sobre las actualizaciones de seguridad.
- Restringir el acceso físico a los dispositivos.
- Monitorear el uso de privilegios, para mitigar aún más los riesgos.

Fuente de Información:	• hxxps://gbhackers.com/teamviewer-clients-vulnerability/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°026	Fecha: 31-01-2025 Página: 5 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en la plataforma de conectividad KEPServerEX de Rockwell Automation		
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 consumo incontrolado de recursos que afecta a la plataforma de conectividad KEPServerEX de Rockwell Automation. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto provocar caídas de los dispositivos, lo que interrumpe las operaciones en los sistemas de control industrial.

2. DETALLES:

KEPServerEX, desarrollado por PTC y ofrecido a través de Rockwell Automation, es una plataforma de conectividad industrial líder diseñada para facilitar la comunicación entre diversos dispositivos de automatización y aplicaciones de software. Sirve como una herramienta vital para integrar diferentes protocolos y sistemas dentro de los entornos de fabricación.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2023-3825 de tipo consumo incontrolado de recursos que afecta a KEPServerEX, podría permitir a un atacante remoto provocar caídas de los dispositivos, lo que interrumpe las operaciones en los sistemas de control industrial.

Múltiples versiones de KEPServerEX son vulnerables a que se les obligue a leer un objeto definido de forma recursiva, lo que conduce a un consumo descontrolado de recursos. KEPServerEX utiliza OPC UA, un protocolo que define varios tipos de objetos que se pueden anidar para crear matrices complejas. No implementa una comprobación para ver si dicho objeto está definido de forma recursiva, por lo que un ataque podría enviar un mensaje creado de forma maliciosa que el decodificador intentaría decodificar hasta que la pila se desbordara y el dispositivo dejara de funcionar.

A. Productos afectados:

- KEPServerEX Versiones 6.0 - 6.14.263.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Actualizar software de todas las instancias de KEPServerEX actualizadas a la versión 6.15 o posterior, que contiene correcciones para esta vulnerabilidad.
- Colocar KEPServerEX en un segmento de red restringido para limitar el acceso solo a dispositivos y personal de confianza.
- Revisar periódicamente los registros del sistema en busca de actividades anormales que puedan indicar un intento de explotación.
- Realizar auditorías de todos los dispositivos que utilizan KEPServerEX para garantizar el cumplimiento e identificar aquellos que sigan siendo vulnerables.
- Brindar capacitación sobre las mejores prácticas de ciberseguridad para que el personal genere conciencia sobre posibles vulnerabilidades.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-030-04

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°026	Fecha: 31-01-2025
		Página: 6 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de autenticación incorrecta en Confluence Data Center		
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:

Atlassian ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo autenticación incorrecta que afecta a Confluence Server y Data Center. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado comprometer el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2023-22515 de tipo autenticación incorrecta en Confluence Data Center, podría permitir a un atacante remoto no autenticado comprometer el sistema afectado.

La vulnerabilidad existe debido a la falta de autenticación en el punto final "/setup/setupadministrator.action". Un atacante remoto no autenticado puede enviar solicitudes especialmente diseñadas al servidor para crear una cuenta administrativa y obtener acceso no autorizado al sistema.

Los atacantes explotan esta vulnerabilidad inyectando configuraciones maliciosas que les permiten acceder a puntos finales de configuración sensibles sin autenticación. Se ha observado que esta vulnerabilidad fue explotada activamente como un día cero, lo que significa que fue utilizada por los atacantes antes de que hubiera un parche disponible.

Hay scripts disponibles en plataformas como GitHub diseñados específicamente para explotar CVE-2023-22515. Estos scripts permiten a los usuarios atacar instancias vulnerables de Confluence de forma individual o en masa, lo que demuestra la facilidad de explotación y el potencial de ataques generalizados.

A. Productos afectados:

- Confluence Data Center: 8.0.0, 8.0.1, 8.0.2, 8.0.3, 8.0.4, 8.1.0, 8.1.1, 8.1.3, 8.2.0, 8.2.1, 8.2.2, 8.2.3, 8.3.0, 8.3.1, 8.3.2, 8.4.0, 8.4.1, 8.4.2, 8.5.0, 8.5.1.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad. Atlassian publicó un aviso el 4 de octubre de 2023, instando a los usuarios a actualizar sus instancias de inmediato o implementar mitigaciones para protegerse contra una posible explotación.

Fuente de Información:	• hxxps://jira.atlassian.com/browse/CONFSERVER-92457 • hxxps://confluence.atlassian.com/display/KB/FAQ+for+CVE-2023-22515 • hxxps://confluence.atlassian.com/pages/viewpage.action?pageId=1295682276 • hxxps://confluence.atlassian.com/security/cve-2023-22515-privilege-escalation-vulnerability-in-confluence-data-center-and-server-1295682276.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°026	Fecha: 31-01-2025
		Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el software de Fortinet		
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 omisión de autenticación que afecta a FortiOS y FortiProxy. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir la autenticación y obtener privilegios de superadministrador en el sistema.

2. DETALLES:

Fortinet, Inc. es una empresa de ciberseguridad que desarrolla y vende soluciones de seguridad como firewalls, seguridad de endpoints y sistemas de detección de intrusos.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-55591 de tipo omisión de autenticación que afecta a FortiOS y FortiProxy, podría permitir a un atacante remoto no autenticados obtener privilegios de superadministrador explotando el módulo websocket de Node.js a través de paquetes especialmente diseñados. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir la autenticación y obtener privilegios de superadministrador en el sistema.

Los actores de amenazas explotan esta vulnerabilidad mediante la creación de nuevas cuentas administrativas con nombres de usuario generados aleatoriamente, que luego utilizan para modificar la configuración del firewall y crear grupos de usuarios de VPN SSL para el acceso no autorizado a redes internas.

Las organizaciones que utilizan versiones vulnerables de los productos Fortinet deben priorizar estas actualizaciones y medidas de seguridad para protegerse contra la posible explotación de esta vulnerabilidad.

A. Productos afectados:

- FortiOS, versiones 7.0.0 hasta la 7.0.16.
- FortiProxy, versiones 7.0.0 a 7.0.19, 7.2.0 a 7.2.12.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Actualizar a las versiones fijas de FortiOS y FortiProxy.
- Limitar el acceso a las interfaces de administración restringiendo las direcciones IP que pueden conectarse.
- Habilitar la MFA para las cuentas de usuarios locales para mejorar la seguridad.
- Implementar una supervisión activa de los registros en busca de actividades sospechosas relacionadas con intentos de acceso no autorizados.
- Supervisar activamente los registros para detectar actividad sospechosa relacionada con intentos de acceso no autorizado.

Fuente de Información:	• hxxps://www.fortiguard.com/psirt/FG-IR-24-535

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°026	Fecha: 31-01-2025 Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en el plugin Sandbox para WordPress		
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 dos vulnerabilidades de severidad **MEDIA** de tipo Scripting entre sitios y autorización faltante en el plugin Sandbox para WordPress. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado eludir los controles de autorización y realizar ataques de secuencias de comandos entre sitios (XSS).

2. DETALLES:

La vulnerabilidad de severidad **baja** identificada por MITRE como CVE-2024-13366 de tipo Scripting entre sitios, podría permitir a un a un atacante remoto realizar ataques de XSS. La vulnerabilidad existe debido a una limpieza insuficiente de los datos proporcionados por el usuario en el parámetro "debug". Un atacante remoto puede engañar a la víctima para que siga un enlace especialmente diseñado y ejecute código HTML y script arbitrario en el navegador del usuario en el contexto de un sitio web vulnerable. La explotación exitosa de esta vulnerabilidad puede permitir a un atacante remoto robar información potencialmente confidencial, cambiar la apariencia de la página web, realizar ataques de phishing y descargas automáticas.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-13367 de tipo autorización faltante en el plugin Sandbox, podría permitir a un atacante remoto eludir los controles de autorización. La vulnerabilidad existe debido a que falta una comprobación de capacidad en la acción "export_download". Un usuario remoto puede descargar una copia completa de un entorno de pruebas y obtener acceso a información confidencial.

A. Productos afectados:

- Sandbox: 0.1 - 0.4.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan estas vulnerabilidades.

Fuente de Información:	• hxxp://wordpress.org/plugins/sandbox/ • hxxp://plugins.trac.wordpress.org/browser/sandbox/trunk/sandbox-ajax.php#L21 • hxxp://www.wordfence.com/threat-intel/vulnerabilities/id/59880d92-5d75-432f-9fb5-d74b13d101ff?source=cve • hxxp://www.wordfence.com/threat-intel/vulnerabilities/id/3fc752bb-3f1d-4106-9df1-361564905a55?source=cve

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°026	Fecha: 31-01-2025 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de divulgación de información 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 **ALTA** de tipo exposición de información confidencial a un actor no autorizado que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener acceso a información potencialmente confidencial.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-43451 de tipo exposición de información confidencial a un actor no autorizado que afecta a varios de sus productos, podría permitir a un atacante remoto no autenticado obtener acceso a información potencialmente confidencial.

La vulnerabilidad existe debido a la divulgación del hash NTLMv2 de un usuario. Un atacante remoto puede engañar a la víctima para que visite un sitio web especialmente diseñado y robar hashes NTLMv2 con una interacción mínima del usuario, lo que puede facilitar otros ataques, como los ataques de paso de hash. Tener en cuenta que esta vulnerabilidad viene siendo explotada activamente en la naturaleza.

La vulnerabilidad se ha utilizado junto con otros programas maliciosos, como SparkRAT, lo que permite a los atacantes controlar de forma remota los sistemas afectados.

A. Productos afectados:

- Múltiples versiones de sistemas Microsoft Windows y Windows Server.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Mejorar la supervisión del tráfico SMB, ya que suele estar menos analizado en comparación con otros protocolos como HTTP o HTTPS.
- Concientizar a los usuarios sobre los riesgos asociados con la apertura o interacción con archivos desconocidos puede ayudar a reducir la probabilidad de explotación.

Fuente de Información:	• hxxps://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-43451

Índice alfabético