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

# 082-2025-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°082 | Fecha: 05-03-2025 |
|---|---|---|
| | | Página: 4 de 5 |

| | | | |
|---|---|---|---|
| Componente que reporta | CENTRO NACIONAL DE SEGURIDAD DIGITAL | | |
| Nombre de la alerta | CrushFTP en riesgo: Vulnerabilidad crítica exponen servidores a ataques | | |
| 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:

CrushFTP, una de las plataformas más utilizadas para la transferencia segura de archivos, está en el centro de una alerta de seguridad tras descubrirse una vulnerabilidad crítica que ya está siendo explotada activamente por atacantes. Esta falla, recientemente revelada, permite a los ciberdelincuentes obtener acceso no autorizado a los servidores afectados, comprometiendo potencialmente datos sensibles de empresas y organizaciones.

## 2. DETALLES:

La vulnerabilidad CVE-2025-2825 en CrushFTP ha sido clasificada con una criticidad alta debido a su impacto y facilidad de explotación. El fallo radica en un problema de autenticación y gestión de permisos, lo que permite a un atacante remoto ejecutar comandos arbitrarios en el servidor sin necesidad de credenciales válidas.

El exploit aprovecha una deficiencia en la validación de las solicitudes enviadas al servidor, lo que permite eludir mecanismos de seguridad y obtener privilegios elevados dentro del sistema. Como resultado, los atacantes pueden acceder, modificar, eliminar o incluso cifrar archivos almacenados en servidores vulnerables.

Si esta vulnerabilidad no es corregida a tiempo, las empresas que utilizan CrushFTP pueden enfrentar los siguientes riesgos:

- **Filtración de datos sensibles:** Acceso no autorizado a información privada o confidencial.
- **Manipulación de archivos:** Modificación, eliminación o cifrado de datos esenciales.
- **Uso del servidor como punto de ataque:** Los atacantes podrían utilizar servidores comprometidos para lanzar ataques contra otras redes.
- **Interrupción de operaciones:** Posible denegación de servicio o pérdida de acceso a archivos críticos.

Uno de los factores más alarmantes es que un exploit funcional ya ha sido publicado en foros y repositorios en línea, lo que ha facilitado que grupos de atacantes comiencen a aprovechar esta vulnerabilidad de forma masiva. Se han identificado intentos de ataque en diversos entornos, para comprometer servidores vulnerables.

## 3. RECOMENDACIONES:

- Actualizar CrushFTP a la última versión que la empresa ha lanzado para corregir esta vulnerabilidad, de inmediato.
- Configurar reglas de firewall para permitir solo conexiones desde direcciones IP confiables.
- Revisar registros del sistema en busca de intentos de acceso no autorizado o ejecución de comandos sospechosos.
- Activar el doble factor de autenticación en todo donde sea posible.
- Deshabilitar funciones innecesarias.
- Revisar configuraciones y permisos de usuario, de tal manera que sólo tengan lo mínimo necesario.
- Establecer un plan de respuesta ante incidentes para actuar rápidamente en caso de una intrusión detectada.

| | |
|---|---|
| Fuente de Información: | • hxxps://devel.group/blog/crushftp-en-riesgo-vulnerabilidad-critica-expone-servidores-a-ataques/ |

# Índice alfabético