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

141-2025-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°141	Fecha: 18-06-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Los dominios confiables se convierten en vectores de amenaza para Phishing		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Las campañas de phishing más efectivas de hoy no se basan únicamente en correos electrónicos falsos o dominios sospechosos. Explotan algo mucho más insidioso: la confianza en las herramientas y servicios que usamos a diario, lo que da lugar al phishing de hora cero.

2. DETALLES:

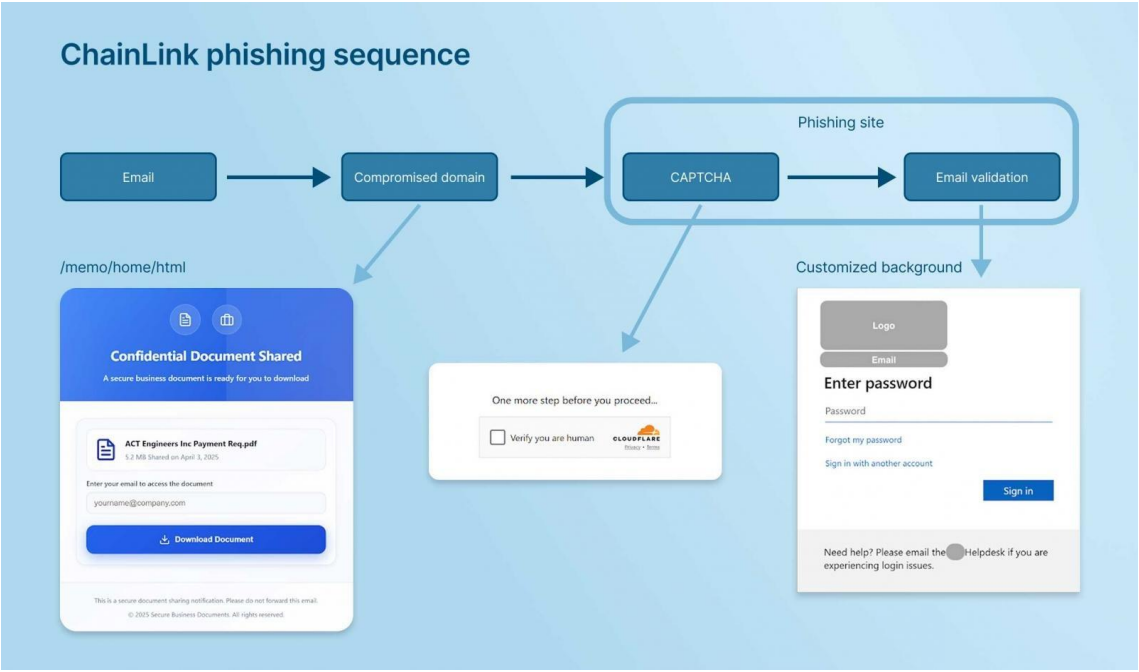
El phishing tradicional se basaba en señales de alerta fácilmente identificables, como remitentes sospechosos y URL dudosas. Pero el phishing moderno ha evolucionado.

Los atacantes ahora canalizan a la víctima desde el correo electrónico a través de una infraestructura confiable antes de recolectar las credenciales.

Un empleado podría recibir un enlace de lo que parece ser Google Drive o Dropbox. A primera vista, no hay nada inusual. Pero tras el clic inicial, el usuario es guiado discretamente a través de una serie de mensajes, cada uno de ellos aparentemente creíbles en sitios web de confianza, hasta que, sin saberlo, entrega credenciales esenciales de la empresa a un atacante.

Esta técnica, que llamamos ChainLink Phishing, se basa en el aprovechamiento de plataformas legítimas y dominios confiables que las herramientas empresariales permiten y que los equipos de seguridad de TI desconocen.

Al usar enlaces legítimos, pasar controles de autenticación de correo electrónico e incluso insertar CAPTCHAs en el camino, los atacantes eluden las defensas tradicionales y permiten que el phishing de hora cero tenga éxito sin ser detectado.



Ejemplo de phishing de ChainLink que aprovecha un dominio comprometido.

Los CAPTCHA y los pasos de verificación son ahora tan comunes en la navegación diaria que los atacantes los explotan como tácticas de ingeniería social, no sólo en campañas de phishing, sino también en otras amenazas basadas en navegador como ClickFix.

Para abordar realmente amenazas como el phishing de ChainLink, debemos ir más allá de las listas de bloqueo estáticas y el filtrado por dominio. El futuro de la protección contra el phishing reside en el análisis en tiempo real de las páginas web y las interacciones de los usuarios con ellas.

Un enlace de phishing que proviene de un servicio confiable suele eludir los filtros de correo electrónico y red. El tráfico al sitio de phishing se permite sin obstáculos porque el dominio no está en una fuente de inteligencia y su reputación no se ve afectada. Y como no se implementa malware, solo se recopilan credenciales, las herramientas de endpoint no tienen nada que detectar.

Los ataques de phishing de ChainLink representan un nuevo nivel de sofisticación, aprovechando la infraestructura confiable para sortear filtros y soluciones de seguridad. Para combatir estas amenazas modernas, es necesario abandonar el enfoque perimetral clásico y actuar directamente donde se manifiesta el riesgo: en el navegador y durante las interacciones del usuario.

El navegador web se ha convertido en el núcleo de la actividad digital empresarial. Desde revisiones de código hasta tareas administrativas, la mayoría de las acciones del día a día suceden en pestañas del navegador. Esta centralización ofrece una superficie de ataque ideal para los actores maliciosos.

3. RECOMENDACIONES:

- Activar el doble factor de autenticación en todo donde sea posible.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Aplicar políticas de contraseñas seguras. Cambiar las contraseñas de todas sus cuentas de manera periódica utilizando una contraseña fuerte y única para cada sitio.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Trasladar la seguridad al punto de interacción real: el navegador.
- Adoptar herramientas capaces de realizar análisis en tiempo real de las páginas web, supervisar el comportamiento del usuario y detectar secuencias encadenadas de phishing antes de que se produzca la filtración de datos.
- Implementar soluciones de protección del navegador que analicen el contenido renderizado.
- Supervisar interacciones en tiempo real y comportamiento contextual del usuario.
- Considerar tecnologías que identifican y bloquean formularios de recolección sospechosos, incluso en dominios conocidos.
- Educar a los empleados sobre los nuevos vectores de ataque que ya no presentan "banderas rojas" evidentes.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/chainlink-phishing-how-trusted-domains-become-threat-vectors/ • hxxps://underc0de.org/foro/noticias-informaticas-120/phishing-de-chainlink-la-nueva-amenaza-que-elude-las-defensas-tradicionales/ • hxxps://www.redeszone.net/noticias/seguridad/phishing-marcas-conocidas-problema/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°141	Fecha: 18-06-2025 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el software Veeam Backup & Replication		
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 Veeam ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo escalada de privilegios que afecta al software Veeam Backup & Replication. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución remota de código (RCE) en el servidor de respaldo por parte de un usuario de dominio autenticado.

2. DETALLES:

Veeam Backup & Replication es una solución de protección de datos probada que ofrece backup y recuperación fiable y eficiente para entornos virtuales, físicos, NAS y nativos de la nube.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-23121 de tipo escalada de privilegios que afecta al software Veeam Backup & Replication, podría permitir a un atacante remoto no autenticado la ejecución remota de código (RCE) en el servidor de respaldo por parte de un usuario de dominio autenticado. Esta vulnerabilidad solo afecta a los servidores de respaldo unidos al dominio.

La explotación requiere una cuenta de usuario de dominio autenticada. La vulnerabilidad afecta específicamente a los servidores de respaldo que están unidos a un dominio, una configuración que Veeam desaconseja pero que sigue siendo común en entornos del mundo real. Un ataque exitoso permite la ejecución remota de código arbitrario en el servidor de respaldo, lo que podría provocar la vulneración total del sistema.

A. Productos afectados:

- Veeam Backup & Replication, versiones 12, 12.1, 12.2, 12.3, 12.3.1 (incluida la compilación 12.3.1.1139 y anteriores).

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- No exponer Veeam Backup & Replication directamente a Internet ni debe estar unido a un dominio para minimizar la superficie de ataque.
- Evaluar las implementaciones de software de Veeam.
- Monitorear los canales de seguridad del proveedor para obtener orientación oficial.
- Implementar la segmentación de la red para limitar la superficie de ataque potencial.
- Considerar el aislamiento temporal o el acceso restringido a los sistemas Veeam afectados hasta que haya un parche disponible.

Fuente de Información:	• hxxps://www.veeam.com/kb4743 • hxxps://www.veeam.com/kb4696 • hxxps://vuldb.com/?id.313156

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°141	Fecha: 18-06-2025 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en las consolas ProGauge MagLink LX de Dover Fueling Solutions		
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:

Dover Fueling Solutions ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo autenticación faltante para función crítica que afecta a las consolas ProGauge MagLink LX, utilizadas para la monitorización de tanques de combustible y agua en los sectores de transporte e infraestructura a nivel mundial. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener el control del dispositivo de monitoreo, manipular las operaciones de abastecimiento de combustible, eliminar la configuración del sistema e implementación de algún tipo de malware.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-5310 de tipo autenticación faltante para función crítica que afecta a la consola ProGauge MagLink LX. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener el control del dispositivo de monitoreo, manipular las operaciones de abastecimiento de combustible, eliminar la configuración del sistema e implementar algún tipo de malware.

La vulnerabilidad surge de la falta de autenticación para una función crítica, exponiendo específicamente una interfaz de Marco de Comunicación de Destino (TCF) no documentada ni autenticada en un puerto específico. La interfaz TCF permite a un atacante remoto no autenticado crear, eliminar o modificar archivos en el dispositivo. Esto puede provocar la ejecución remota de código, lo que podría otorgar al atacante control total sobre el dispositivo de monitoreo. Una explotación exitosa podría permitir la manipulación de operaciones de abastecimiento de combustible, la eliminación de configuraciones del sistema o la implementación de malware.

A. Productos afectados:

- ProGauge MagLink LX 4: versiones anteriores a la 4.20.3.
- ProGauge MagLink LX Plus: versiones anteriores a la 4.20.3.
- ProGauge MagLink LX Ultimate: versiones anteriores a la 5.20.3.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Actualizar sus dispositivos ProGauge MagLink a la versión 4.20.3 o posterior, para los modelos MagLink LX 4 y MagLink LX Plus. La actualización se puede descargar desde el sitio web de Dover Fueling Solutions.
- Actualizar a la versión 5.20.3 o posterior, para los dispositivos MagLink LX Ultimate.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-168-05xxx

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°141	Fecha: 18-06-2025
		Página: 8 de 9

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

Citrix Systems, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo lectura fuera de límites que afecta a los productos Citrix NetScaler ADC y NetScaler Gateway. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la exposición de datos confidenciales de memoria (credenciales, configuración).

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-5777 de tipo fuera de límites que afecta a los productos Citrix NetScaler ADC y NetScaler Gateway. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la exposición de datos confidenciales de memoria (credenciales, configuración).

La vulnerabilidad existe debido a una validación de entrada insuficiente, lo que provoca una condición de sobrelectura de memoria. Esta falla puede explotarse remotamente sin autenticación, lo que permite a los atacantes leer contenido confidencial de la memoria, incluyendo credenciales y datos de configuración, lo que supone un grave riesgo para la confidencialidad, la integridad y la disponibilidad de los sistemas afectados.

A. Productos afectados:

- NetScaler ADC y NetScaler Gateway 14.1, versiones anteriores a la 14.1-43.56.
- NetScaler ADC y NetScaler Gateway 13.1, versiones anteriores a la 13.1-58.32.
- NetScaler ADC 13.1-FIPS y NDcPP, versiones anteriores a 13.1-37.235-FIPS y NDcPP.
- NetScaler ADC 12.1-FIPS, versiones anteriores a 12.1-55.328-FIPS.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Auditar y restringir inmediatamente el acceso de red a la interfaz de administración de NetScaler.
- Aplicar las actualizaciones de seguridad recomendadas por el proveedor cuando estén disponibles.
- Implementar la segmentación de red para limitar la exposición.
- Monitorear cualquier actividad de red sospechosa dirigida a NetScaler ADC y NetScaler Gateway.
- Realizar una evaluación de seguridad exhaustiva de todas las implementaciones de NetScaler.

Fuente de Información:	• hxxps://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420

Índice alfabético