



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

## 002-2026-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 Aérea del 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 las empresas 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

Un ataque a la cadena de suministro aprovecha el mecanismo de actualización de Notepad++ para distribuir malware dirigido..... 4

Vulnerabilidad de secuencias de comandos entre sitios almacenadas en FacturaScripts. .... 6

Vulnerabilidad en el software de diseño de sitios web de Ankara Hosting..... 7

Índice alfabético ..... 8

	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°002</b>		Fecha: 03-02-2026
			Página: 4 de 8
<b>Componente que reporta</b>	<b>CENTRO NACIONAL DE SEGURIDAD DIGITAL</b>		
<b>Nombre de la alerta</b>	Un ataque a la cadena de suministro aprovecha el mecanismo de actualización de Notepad++ para distribuir malware dirigido.		
<b>Tipo de Ataque</b>	malware	<b>Abreviatura</b>	malware
<b>Medios de propagación</b>	Correo electrónico, redes sociales, entre otros		
<b>Código de familia</b>	C	<b>Código de Sub familia</b>	C02
<b>Clasificación temática familia</b>	Código Malicioso		

**Descripción**

**1. ANTECEDENTES:**

Notepad++, uno de los editores de texto más utilizados en entornos técnicos y administrativos, fue afectado por un ataque sofisticado a su cadena de suministro cuando actores maliciosos comprometieron la infraestructura del proveedor de alojamiento responsable del sistema de actualizaciones. Esta intrusión permitió manipular el canal de actualización oficial durante varios meses (entre junio y diciembre de 2025), sin necesidad de vulnerar el código fuente de la aplicación, aprovechando debilidades en los mecanismos de verificación criptográfica del actualizador WinGUP en versiones antiguas. Investigaciones independientes y comunicados oficiales señalaron que el ataque fue altamente selectivo y atribuido con alta probabilidad a un actor patrocinado por un Estado, lo que evidencia un interés estratégico más allá del lucro económico tradicional.



*Ilustración 1: Un ataque a la cadena de suministro aprovecha el mecanismo de actualización de Notepad++ para distribuir malware dirigido.*

**2. DETALLES:**


El ataque se materializó cuando los operadores lograron acceso al servidor de hosting que alojaba el servicio `getDownloadUrl.php`, interceptando y redirigiendo solicitudes legítimas de actualización de Notepad++ hacia servidores controlados por los atacantes, desde donde se distribuían instaladores maliciosos firmemente diseñados para pasar inadvertidos. El compromiso inicial ocurrió en junio de 2025; aunque el atacante perdió acceso directo tras una actualización de kernel del proveedor en septiembre, conservó credenciales internas que le permitieron continuar el secuestro del tráfico hasta diciembre de ese año. Las cargas distribuidas incluían instaladores NSIS con capacidades de reconocimiento del sistema y despliegue de implants avanzados, dirigidos únicamente a víctimas específicas, principalmente en sectores estratégicos. Tras la detección pública, el proyecto migró su infraestructura, rotó credenciales y lanzó la versión 8.8.9 con controles reforzados de validación de firma y certificado, mitigando el vector de ataque.


### 3. RECOMENDACIONES:

- Mantener el software actualizado únicamente desde fuentes oficiales y verificadas, evitando descargas desde enlaces, avisos emergentes o repositorios no institucionales.
- Adoptar una gestión centralizada de actualizaciones en organizaciones, reduciendo la dependencia de mecanismos automáticos individuales.
- Reforzar la concientización del usuario sobre que incluso herramientas legítimas pueden ser utilizadas como vector de ataque cuando su cadena de distribución es comprometida.
- Implementar defensa en profundidad, entendiendo que la confianza en proveedores de software debe complementarse con controles internos de seguridad.
- Asegurar que exista un plan de respuesta a incidentes que contemple escenarios de compromiso de software confiable.
- Promover una cultura de verificación y cautela digital, incluso frente a aplicaciones ampliamente utilizadas y de buena reputación.

Fuente de Información:

- <https://gbhackers.com/interlock-ransomware/>

	<b>ALERTA DE SEGURIDAD DIGITAL N°056</b>		Fecha: 03-02-2026
			Página: 6 de 8
<b>Componente que reporta</b>	<b>DIRECCIÓN NACIONAL DE INTELIGENCIA</b>		
<b>Nombre de la alerta</b>	Vulnerabilidad de secuencias de comandos entre sitios almacenadas en FacturaScripts.		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC
<b>Medios de propagación</b>	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
<b>Código de familia</b>	H	<b>Código de Sub familia</b>	H01
<b>Clasificación temática familia</b>	Intento de intrusión		
<b>Descripción</b>			
<p><b>1. ANTECEDENTES:</b></p> <p>Se ha publicado una vulnerabilidad de severidad <b>MEDIA</b> clasificada como CWE-79: Neutralización incorrecta de la entrada durante la generación de páginas web (Cross-site Scripting) que afecta a FacturaScripts. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado realizar ataques de secuencias de comandos entre sitios (XSS).</p> <p><b>2. DETALLES:</b></p> <p>La vulnerabilidad de severidad <b>media</b> identificada por MITRE como <a href="#">CVE-2026-23997</a> de tipo CWE-79: Neutralización incorrecta de la entrada durante la generación de páginas web (Cross-site Scripting) que afecta al software FacturaScripts, que es un sistema ERP (Enterprise Resource Planning) y de contabilidad de código abierto. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado realizar ataques de secuencias de comandos entre sitios (XSS).</p> <p>La vulnerabilidad existe debido a una limpieza insuficiente de los datos proporcionados por el usuario en el campo "Observaciones" de la Vista del Historial. Un usuario remoto puede inyectar y ejecutar código HTML y script arbitrario en el navegador del usuario en el contexto de un sitio web vulnerable.</p> <p>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 de descarga automática.</p> <p><b>A. Productos afectados:</b></p> <ul style="list-style-type: none"> <li>– FacturaScripts, versiones 2025.71 y anteriores (hasta la versión afectada).</li> </ul> <p><b>3. RECOMENDACIONES:</b></p> <ul style="list-style-type: none"> <li>• Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.</li> </ul>			
<b>Fuente de Información:</b>		<ul style="list-style-type: none"> <li>• <a href="https://github.com/NeoRazorX/facturascripts/security/advisories/GHSA-4v7v-7v7r-3r5h/#poc">hxxps://github.com/NeoRazorX/facturascripts/security/advisories/GHSA-4v7v-7v7r-3r5h/#poc</a></li> </ul>	

	<b>ALERTA DE SEGURIDAD DIGITAL N°057</b>		Fecha: 03-02-2026
			Página: 7 de 8
<b>Componente que reporta</b>	<b>DIRECCIÓN NACIONAL DE INTELIGENCIA</b>		
<b>Nombre de la alerta</b>	Vulnerabilidad en el software de diseño de sitios web de Ankara Hosting.		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC
<b>Medios de propagación</b>	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
<b>Código de familia</b>	H	<b>Código de Sub familia</b>	H01
<b>Clasificación temática familia</b>	Intento de intrusión		
<b>Descripción</b>			
<p><b>1. ANTECEDENTES:</b></p> <p>Ankara Hosting ha publicado una vulnerabilidad de severidad <b>ALTA</b> clasificada como CWE-79: Neutralización incorrecta de la entrada durante la generación de páginas web (Cross-site Scripting) en el software de diseño de sitios web de Ankara Hosting. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado inyectar scripts maliciosos que se ejecutan en los navegadores de los usuarios al visitar URL manipuladas.</p> <p><b>2. DETALLES:</b></p> <p>La vulnerabilidad de severidad <b>alta</b> identificada por MITRE como <a href="#">CVE-2026-6397</a> de CWE-79: Neutralización incorrecta de la entrada durante la generación de páginas web (Cross-site Scripting) en el software de diseño web de Ankara Hosting, podría permitir a un atacante remoto no autenticado inyectar scripts maliciosos que se ejecutan en los navegadores de los usuarios al visitar URL manipuladas. Esto podría provocar el secuestro de sesiones, el robo de credenciales, la distribución de malware o la desfiguración del sitio web.</p> <p>La vulnerabilidad puede explotarse remotamente sin necesidad de autenticación ni privilegios especiales, aunque sí se requeriría la interacción del usuario para hacer clic en un enlace malicioso. Dado el alto nivel de impacto en la disponibilidad, esto podría aprovecharse para provocar condiciones de denegación de servicio o el agotamiento de los recursos del sistema.</p> <p><b>A. Productos afectados:</b></p> <ul style="list-style-type: none"> <li>– Sistema de diseño de sitio web de Ankara Hosting Website Design Website Software en versiones hasta 03/02/2026.</li> </ul> <p><b>B. Indicadores de compromiso (IoC):</b></p> <ul style="list-style-type: none"> <li>– Registros de servidor con solicitudes HTTP que contienen parámetros con contenido JavaScript inusual (por ejemplo &lt;script&gt;...&lt;/script&gt;), especialmente en URLs repetidas hacia páginas dinámicas.</li> <li>– Alertas de seguridad o WAF que identifiquen patrones de XSS reflejado.</li> <li>– Comportamiento inesperado en sesiones de usuarios que accedieron páginas con parámetros manipulados.</li> </ul> <p><b>3. RECOMENDACIONES:</b></p> <ul style="list-style-type: none"> <li>• Implementar una validación de entrada y una codificación de salida estrictas para todos los datos proporcionados por el usuario.</li> <li>• Utilizar una codificación adecuada al contexto (HTML, JavaScript, URL) al reflejar la entrada del usuario en las páginas web.</li> <li>• Implementar encabezados de la Política de Seguridad de Contenido (CSP) para restringir la ejecución de scripts.</li> <li>• Aplicar reglas de Firewall de Aplicaciones Web (WAF) para detectar y bloquear intentos de XSS.</li> <li>• Evitar hacer clic en enlaces sospechosos.</li> <li>• Supervisar los intentos de explotación y los informes de usuarios sobre comportamientos inusuales.</li> <li>• Dada la falta de respuesta del proveedor, considerar evaluar soluciones alternativas o implementar controles compensatorios hasta que haya un parche disponible.</li> </ul>			
<b>Fuente de Información:</b>		<ul style="list-style-type: none"> <li>• <a href="https://www.usom.gov.tr/bildirim/tr-26-0014">https://www.usom.gov.tr/bildirim/tr-26-0014</a></li> </ul>	

## Índice alfabético

malware .....	4
Explotación de vulnerabilidades conocidas .....	6,7