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

008-2026-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 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°008	Fecha: 11-02-2026
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La nueva campaña RAT de XWorm aprovecha el phishing y el exploit de Excel CVE-2018-0802 para eludir la detección.		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

De acuerdo con GBHackers, una campaña activa entrega una variante reciente de XWorm—un RAT modular en .NET comercializado desde 2022—mediante correos temáticos de negocio (pagos, órdenes de compra, documentos bancarios) que adjuntan un add-in de Excel (.XLAM); el archivo abusa de un objeto OLE para activar CVE-2018-0802 (Equation Editor) y desplegar una cadena multietapa difícil de detectar. XWorm ofrece control remoto completo, exfiltración de credenciales/cookies, capacidades de DDoS y hasta ransomware, lo que mantiene su alta demanda en foros criminales.

Ilustración 1: La nueva campaña RAT de XWorm aprovecha el phishing y el exploit de Excel CVE-2018-0802 para eludir la detección.

2. DETALLES:

La intrusión inicia con phishing que induce a abrir un .XLAM; al cargarse, el Equation Editor procesa un OLE especialmente formado y ejecuta shellcode que descarga un HTA ofuscado y lo lanza con mshta.exe. Ese HTA desencripta y dispara PowerShell que recupera una imagen JPEG con un módulo .NET oculto entre marcadores; el módulo se inyecta en memoria (sin tocar disco) y actúa como loader de XWorm, descifrando configuración y conectando a una URL C2 para traer el payload final. Para evasión, la cadena usa living-off-the-land (mshta/PowerShell) y proceso hollowing (p. ej., Msbuild.exe), además de cifrado en el canal de C2. El uso de la CVE-2018-0802—aun parcheada desde 2018—expone brechas de higiene de parches y explica su vigencia en campañas actuales, según el análisis técnico de FortiGuard.

3. RECOMENDACIONES:

- Patching urgente: verificar y aplicar mitigaciones/hotfix de CVE-2018-0802 en Office heredado; endurecer políticas de OLE/macros y bloqueo de .XLAM provenientes de correo.
- Controles de ejecución (hardening): restringir/alertar uso de mshta.exe, PowerShell, Msbuild.exe desde contextos de usuario y adjuntos; aplicar AMSI y reglas de Constrained Language Mode donde sea viable.
- Correo y web: reforzar gateway con detección de OLE/HTA, link-sandboxing y políticas anti-phishing; someter .XLAM/ZIP/HTA a análisis estático-dinámico antes de entrega al usuario.
- EDR/XDR y hunting: crear detecciones para cadena Excel→Equation Editor→mshta→PowerShell→Msbuild, carga Base64 y descifrado en memoria; vigilar beaconing cifrado y dominios C2 citados por la investigación.
- Segmentación y mínimos privilegios: limitar alcance de cuentas/hosts con acceso a documentación financiera (blancos de los señuelos); aplicar listas de aplicaciones permitidas (WDAC/AppLocker).
- Respuesta y contención: ante indicios, aislar el endpoint, terminar mshta/PowerShell/Msbuild anómalos, revocar credenciales y bloquear IoCs (dominios/URLs/hash); realizar forense de memoria por la naturaleza fileless.

Fuente de Información:	• hxxps://gbhackers.com/spam-and-phishing-report/

	ALERTA DE SEGURIDAD DIGITAL N°073	Fecha: 11-02-2026
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de Inyección de comando que afecta a la aplicación Windows Notepad.		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
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** clasificada como CWE-77: Neutralización incorrecta de elementos especiales utilizados en un comando (Inyección de comando) que afecta a la aplicación Windows Notepad. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante la ejecución remota de código (RCE) a través de una red.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2026-20841 de tipo CWE-77: Neutralización incorrecta de elementos especiales utilizados en un comando (Inyección de comando) que afecta a la aplicación Windows Notepad, podría permitir a un atacante remoto no autenticado ejecutar código a través de una red.

La vulnerabilidad se debe a una inyección de comandos (CWE-77) en el manejo de archivos Markdown, lo que permite a un atacante ejecutar código arbitrario en el sistema de la víctima mediante ingeniería social.

El atacante crea un archivo Markdown malicioso (.md) con enlaces especialmente diseñados. La víctima abre el archivo con Windows Notepad y al interactuar con el enlace, Notepad ejecuta comandos o descarga archivos remotos, de esta forma el atacante obtiene ejecución de código en el contexto del usuario.

El soporte de Markdown, enlaces y funciones de red convierte a Notepad en un vector potencial de RCE, similar a navegadores o editores avanzados, lo que aumenta la superficie de ataque corporativa.

A. Productos afectados:

- Windows Notepad (versiones modernas con soporte Markdown),
- Versiones previas a las actualizaciones de seguridad de febrero 2026,
- Sistemas Windows 10 y Windows 11 con Notepad actualizado desde Microsoft Store.

B. Indicadores de Compromiso (IoC):

- Notepad.exe iniciando procesos hijos (PowerShell, cmd, wscript),
- Descarga de archivos tras abrir Markdown,
- Actividad de red iniciada por Notepad hacia dominios desconocidos.

3. RECOMENDACIONES:

- Aplicar parches de seguridad de Microsoft (Patch Tuesday febrero 2026),
- Actualizar Notepad a versiones corregidas,
- Deshabilitar apertura automática de enlaces en Markdown,
- Filtrar archivos .md en campañas de correo,
- Implementar sandboxing para aplicaciones de usuario,
- Monitorear procesos sospechosos generados por Notepad (cmd.exe, powershell.exe).

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20841 • hxxps://news.ycombinator.com/item?id=46971516

	ALERTA DE SEGURIDAD DIGITAL N°074	Fecha: 11-02-2026
		Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de omisión de funciones de seguridad del shell de Windows.		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
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** clasificada como CWE-693: Falla del mecanismo de protección que afecta a múltiples versiones de Windows y Windows Server. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir las restricciones de seguridad implementadas.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2026-21510 de tipo CWE-693: Falla del mecanismo de protección que afecta a múltiples versiones de Windows y Windows Server, podría permitir a un atacante remoto no autenticado eludir las restricciones de seguridad implementadas. Para explotar con éxito esta vulnerabilidad, un atacante debe convencer a un usuario de que abra un enlace malicioso o un archivo de acceso directo.

La vulnerabilidad existe debido a la implementación insuficiente de medidas de seguridad. Un atacante puede engañar a la víctima para que haga clic en una URL o un archivo de acceso directo especialmente diseñado para eludir las indicaciones de seguridad de Windows SmartScreen y Windows Shell y ejecutar código arbitrario en el sistema. Esta vulnerabilidad se está explotando activamente en la naturaleza.

A. Productos afectados:

- Windows, Windows Server, múltiples versiones

3. RECOMENDACIONES:

- 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-2026-21510

Índice alfabético