

# ALERTA INTEGRADA DE SEGURIDAD DIGITAL



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

La red FEMITBOT explota las miniaplicaciones de Telegram para propagar estafas de criptomonedas y malware para Android. ....	4
Vulnerabilidad de ejecución remota de código en el servidor Apache HTTP con el protocolo HTTP/2. ....	6
Falsos positivos en Microsoft Defender comprometen la cadena de confianza de certificados digitales en entornos gubernamentales. ....	7
Vulnerabilidad en productos de Cisco. ....	9
Índice alfabético .....	10

 Centro Nacional de Seguridad Digital	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066</b>		Fecha: 06-05-2026
			Página: 4 de 10
<b>Componente que reporta</b>	<b>CENTRO NACIONAL DE SEGURIDAD DIGITAL</b>		
<b>Nombre de la alerta</b>	La red FEMITBOT explota las miniaplicaciones de Telegram para propagar estafas de criptomonedas y malware para Android.		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC
<b>Medios de propagación</b>	Red, Internet		
<b>Código de familia</b>	H	<b>Código de Sub familia</b>	H01
<b>Clasificación temática familia</b>	Intento de intrusión		
<b>Descripción</b>			

**1. ANTECEDENTES:**

En mayo de 2026, investigadores de seguridad identificaron una infraestructura maliciosa a gran escala denominada FEMITBOT, la cual abusa de la funcionalidad Telegram Mini Apps para ejecutar campañas de fraude y malware a nivel global. Esta alerta revela cómo los atacantes están aprovechando funciones legítimas y confiables de plataformas de mensajería para evadir controles tradicionales de seguridad, explotar la confianza del usuario y ejecutar estafas altamente sofisticadas dentro de entornos que aparentan ser seguros y nativos de la aplicación.



*Ilustración 1 La red FEMITBOT explota las miniaplicaciones de Telegram para propagar estafas de criptomonedas y malware para Android.*

**2. DETALLES:**


La red FEMITBOT utiliza bots de Telegram que, al interactuar con el usuario, lanzan Mini Apps maliciosas dentro del navegador embebido (WebView) de Telegram. Estas Mini Apps cargan sitios de phishing que integran el Telegram WebApp SDK, permitiendo a los atacantes recolectar silenciosamente datos del usuario como ID, nombre y tokens de autenticación (initData). Las campañas impersonan marcas reconocidas de los sectores crypto, streaming, IA y servicios financieros, mostrando paneles falsos con balances ficticios y contadores de ganancias para inducir a las víctimas a realizar “depósitos de activación”. Paralelamente, algunas variantes ofrecen descargas de APK maliciosos para Android, facilitando infecciones persistentes. La infraestructura es modular, con decenas de dominios y bots conectados a un backend común que optimiza las estafas mediante herramientas de seguimiento publicitario (Meta y TikTok pixels), elevando el impacto financiero y operativo del ataque.


### 3. RECOMENDACIONES:

- Desconfiar de bots y Mini Apps de Telegram que prometan inversiones rápidas, ingresos pasivos o promociones exclusivas.
- Evitar realizar pagos, depósitos o descargas desde Mini Apps cuya legitimidad no pueda verificarse externamente.
- No instalar APK fuera de Google Play ni habilitar la instalación desde fuentes desconocidas.
- Mantener Android actualizado, junto con Google Play Protect y soluciones antimalware activas.
- Implementar controles de concienciación en ciberseguridad sobre estafas tipo advance-fee y phishing en plataformas de mensajería.
- En entornos corporativos, aplicar Mobile Threat Defense (MTD) y políticas MDM para restringir la ejecución de apps no autorizadas.
- Reportar bots y Mini Apps sospechosas directamente a Telegram para su análisis y desactivación.

**Fuente de Información:**

- <https://gbhackers.com/femitbot-network-exploits-telegram-mini-apps/>

	<b>ALERTA DE SEGURIDAD DIGITAL N°239</b>		Fecha: 06-05-2026
			Página: 6 de 10
<b>Componente que reporta</b>	<b>DIRECCIÓN NACIONAL DE INTELIGENCIA</b>		
<b>Nombre de la alerta</b>	Vulnerabilidad de ejecución remota de código en el servidor Apache HTTP con el protocolo HTTP/2.		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC
<b>Medios de propagación</b>	Red, Internet		
<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>Apache Software Foundation ha reportado una vulnerabilidad de severidad “<b>ALTA</b>” clasificada como CWE-415: Liberación doble de memoria (Double Free) que afecta a Apache HTTP Server 2.4.66. Esta falla permite que un atacante remoto manipule la gestión de memoria del servidor mediante tráfico HTTP/2 especialmente diseñado, lo que puede derivar en denegación de servicio (DoS) o incluso ejecución remota de código (RCE). El riesgo es elevado debido a la amplia adopción de Apache y a que el vector de ataque es remoto sin requerir interacción del usuario.</p> <p><b>2. DETALLES:</b></p> <p>La vulnerabilidad de severidad <b>alta</b> identificada por MITRE como <a href="#">CVE-2026-23918</a> se origina en un error de tipo double free dentro del módulo mod_http2, específicamente en la lógica de limpieza de streams del archivo h2_mplx.c. El fallo se activa cuando un atacante envía una secuencia específica de frames HTTP/2 —un HEADERS seguido de un RST_STREAM con código de error— antes de que el stream sea correctamente registrado por el multiplexor. Esto provoca la liberación doble de memoria, generando corrupción del heap.</p> <p>Desde una perspectiva técnica, CVE-2026-23918 permite que la corrupción de memoria resultante sea explotada para provocar fallos del servicio o, en escenarios más avanzados, manipular estructuras internas del proceso para lograr ejecución de código arbitrario. La vulnerabilidad tiene una puntuación CVSS aproximada de 8.8 (High/Critical), lo que refleja su alto impacto en confidencialidad, integridad y disponibilidad.</p> <p>A la fecha, no existe evidencia pública confirmada de explotación activa en campañas reales. Sin embargo, debido a la criticidad del fallo y la disponibilidad de detalles técnicos, es altamente probable la aparición de exploits funcionales en el corto plazo. No se ha confirmado oficialmente un PoC público plenamente funcional, aunque la naturaleza del bug facilita su desarrollo por actores avanzados. (No puedo confirmar explotación activa en el mundo real más allá de reportes técnicos disponibles).</p> <p>El riesgo es alto a crítico, especialmente para organizaciones que exponen servicios web con HTTP/2 habilitado. La explotación remota sin autenticación, combinada con potencial RCE, convierte esta vulnerabilidad en un vector ideal para ataques masivos, botnets o ransomware. La falta de parcheo inmediato incrementa exponencialmente la superficie de exposición.</p> <p><b>A. Productos afectados:</b></p> <ul style="list-style-type: none"> <li>– Apache HTTP Server 2.4.66.</li> </ul> <p><b>3. RECOMENDACIONES:</b></p> <ul style="list-style-type: none"> <li>• Actualizar inmediatamente a Apache HTTP Server 2.4.67 o superior,</li> <li>• Deshabilitar HTTP/2 si no es estrictamente necesario (mitigación temporal),</li> <li>• Implementar WAF con reglas para anomalías en tráfico HTTP/2,</li> <li>• Monitorizar logs en busca de patrones anómalos de frames HTTP/2,</li> <li>• Aplicar hardening de memoria (ASLR, DEP) y sandboxing del servicio,</li> <li>• Segmentar servicios expuestos y limitar superficie de ataque.</li> </ul>			
<b>Fuente de Información:</b>		<ul style="list-style-type: none"> <li>• <a href="https://www.openwall.com/lists/oss-security/2026/05/04/19">hxxp://www.openwall.com/lists/oss-security/2026/05/04/19</a></li> <li>• <a href="https://httpd.apache.org/security/vulnerabilities_24.html">hxxps://httpd.apache.org/security/vulnerabilities_24.html</a></li> </ul>	

	<b>ALERTA DE SEGURIDAD DIGITAL N°240</b>		<b>Fecha: 06-05-2026</b>
<b>Componente que reporta</b>	<b>DIRECCIÓN NACIONAL DE INTELIGENCIA</b>		
<b>Nombre de la alerta</b>	Falsos positivos en Microsoft Defender comprometen la cadena de confianza de certificados digitales en entornos gubernamentales.		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC
<b>Medios de propagación</b>	Red, Internet		
<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>El 30 de abril de 2026, a nivel global en entornos Windows, Microsoft introdujo una actualización de firmas de seguridad en Microsoft Defender que provocó la detección errónea de certificados raíz legítimos de DigiCert como malware identificado como Trojan:Win32/Cerdigent.A!dha. El incidente fue reportado públicamente el 3 de mayo de 2026 y afectó a organizaciones y administradores de sistemas en múltiples sectores. El problema se originó por una lógica defectuosa en las firmas antivirus, lo que generó falsos positivos masivos y la eliminación automática de certificados críticos del almacén de confianza de Windows.</p> <p>El incidente de falso positivo en Microsoft Defender tiene un impacto particularmente crítico en entidades públicas peruanas, debido a la alta dependencia de infraestructuras Windows y servicios digitales basados en certificados digitales para garantizar autenticidad, integridad y confidencialidad. La eliminación errónea de certificados raíz confiables afecta directamente la validación SSL/TLS, lo que puede interrumpir portales gubernamentales (SUNAT, RENIEC, plataformas de interoperabilidad del Estado, sistemas judiciales, etc.), generando fallas en autenticación y en el establecimiento de conexiones seguras.</p> <p><b>2. DETALLES:</b></p> <p>El evento consistió en la clasificación incorrecta de certificados raíz ampliamente confiables (incluyendo DigiCert Assured ID Root CA y DigiCert Trusted Root G4) como amenazas de alta severidad. Esta detección errónea provocó la remoción de certificados desde el registro del sistema (AuthRoot), afectando la validación de conexiones SSL/TLS y la confianza en firmas digitales. La causa técnica fue una actualización defectuosa de inteligencia de seguridad (Security Intelligence) que introdujo reglas de detección incorrectas asociadas a un contexto previo de certificados comprometidos.</p> <p>El impacto principal se manifestó en la interrupción de servicios críticos, fallas en validación de certificados, generación masiva de alertas falsas y acciones incorrectas por parte de administradores (incluyendo reinstalaciones de sistemas). La amenaza no correspondía a malware real, pero generó un riesgo operativo significativo al degradar la confianza en los mecanismos de seguridad y potencialmente habilitar escenarios donde amenazas reales podrían pasar desapercibidas debido a la fatiga de alertas. Microsoft corrigió el problema mediante actualizaciones posteriores de firmas (versión 1.449.430.0+), restaurando la funcionalidad normal.</p> <p>Este incidente no representa una intrusión, pero sí un riesgo sistémico relevante en la cadena de confianza digital. La eliminación de certificados raíz constituye un vector indirecto de impacto crítico, ya que compromete la base de autenticación de múltiples servicios. Además, la correlación temporal con un incidente real de certificados comprometidos sugiere una sobrecompensación en mecanismos de detección, lo que resalta la necesidad de controles más robustos en la validación de firmas antimalware antes de su despliegue global.</p> <p>Este incidente evidencia una dependencia crítica del Estado peruano en infraestructuras de confianza digital centralizadas (PKI y certificados raíz). Un fallo en la cadena de confianza —aunque sea por error del proveedor— puede generar un efecto cascada sobre múltiples servicios públicos esenciales.</p> <p>El riesgo real no radica únicamente en la interrupción operativa, sino en la posible degradación de controles de seguridad y confianza institucional, lo que podría ser aprovechado por actores de amenaza en escenarios posteriores. En consecuencia, este tipo de eventos debe ser tratado como un incidente de seguridad de alto impacto sistémico, no como un simple falso positivo.</p> <p><b>A. Datos Clave del Incidente:</b></p> <ul style="list-style-type: none"> <li>– Tipo de ataque: Falso positivo / fallo de detección (error en motor AV),</li> <li>– Nivel de criticidad: ALTO (impacto operativo y en confianza criptográfica),</li> </ul>			

- Organización afectada: Usuarios y organizaciones que utilizan Microsoft Defender,
- Productos afectados: Microsoft Defender, Windows (trust store), certificados DigiCert,
- Actor de amenaza: No aplica,
- Impacto: Interrupción de validación TLS, eliminación de certificados raíz, fatiga de alertas, potencial degradación de seguridad,
- Fecha del incidente: 30 de abril – 3 de mayo de 2026.

#### B. Indicadores de Compromiso (IoC):

Nota: No son IoC de intrusión real, sino artefactos asociados al falso positivo:


- Nombre de detección: Trojan:Win32/Cerdigent.A!dha,
- Hashes de certificados afectados: 0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43, DDFB16CD4931C973A2037D3FC83A4D7D775D05E4,
- Ruta de registro afectada: HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates,
- Acción observada: eliminación o cuarentena de certificados raíz.

#### 3. RECOMENDACIONES:

- Actualizar inmediatamente Microsoft Defender a versiones de inteligencia  $\geq 1.449.430.0$
- Verificar integridad del almacén de certificados raíz (AuthRoot)
- Restaurar certificados eliminados automáticamente tras actualización
- Implementar monitoreo de cambios en el trust store de Windows
- Establecer validación cruzada antes de ejecutar acciones destructivas automáticas
- Aplicar controles de gestión de falsos positivos en SOC (playbooks específicos)
- Mantener respaldo de configuraciones PKI en entornos críticos.

#### Fuente de Información:

- <https://www.bleepingcomputer.com/news/security/microsoft-defender-wrongly-flags-digicert-certs-as-trojan-win32-cerdigentadha/>

	<b>ALERTA DE SEGURIDAD DIGITAL N°241</b>		Fecha: 06-05-2026
			Página: 9 de 10
<b>Componente que reporta</b>	<b>DIRECCIÓN NACIONAL DE INTELIGENCIA</b>		
<b>Nombre de la alerta</b>	Vulnerabilidad en productos de Cisco.		
<b>Tipo de Ataque</b>	Explotación de vulnerabilidades conocidas	<b>Abreviatura</b>	EVC
<b>Medios de propagación</b>	Red, Internet		
<b>Código de familia</b>	H	<b>Código de Sub familia</b>	H01
<b>Clasificación temática familia</b>	Intento de intrusión		

**Descripción**

**1. ANTECEDENTES:**

Cisco Systems, Inc. ha publicado una vulnerabilidad de severidad **MEDIA** clasificada como CWE-79: Neutralización incorrecta de la entrada durante la generación de páginas web que afecta a la interfaz de gestión basada en web de Cisco Identity Services Engine (ISE), permitiendo ataques de ejecución de scripts en sitios cruzados (XSS). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto que cuente con credenciales administrativas válidas puede inyectar código JavaScript malicioso en páginas específicas de la plataforma.

**2. DETALLES:**

La vulnerabilidad de severidad **media** identificada por MITRE como [CVE-2025-20205](#) de tipo CWE-79: Neutralización incorrecta de la entrada durante la generación de páginas web que afecta a la interfaz de gestión basada en web de Cisco Identity Services Engine (ISE), permitiendo ataques de ejecución de scripts en sitios cruzados (XSS), podría permitir a un atacante remoto que cuente con credenciales administrativas válidas puede inyectar código JavaScript malicioso en páginas específicas de la plataforma. Cuando otros administradores acceden a estas páginas, el script se ejecuta en su contexto de navegador, lo que puede facilitar el robo de sesiones, la captura de credenciales o la ejecución de acciones administrativas no autorizadas.

**A. Productos afectados:**

- Cisco ISE 3.2.0;
- Cisco ISE 3.3.0;
- Cisco ISE 3.4.0.

**3. RECOMENDACIONES:**

- Actualizar el software de Cisco ISE a la versión con el parche de seguridad correspondiente.
- Restringir el acceso a la interfaz de gestión de ISE únicamente a redes de gestión seguras y personal autorizado.
- Auditar regularmente las cuentas administrativas y limitar el acceso a los privilegios necesarios.
- Implementar la autenticación multifactor (MFA) para proteger todas las cuentas administrativas frente a posibles robos de credenciales.

<b>Fuente de Información:</b>	<ul style="list-style-type: none"> <li>• <a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-42tgsdMG">hxxps[:]//sec[.]cloudapps[.]cisco[.]com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-42tgsdMG</a></li> </ul>
-------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Índice alfabético

Explotación de vulnerabilidades conocidas ..... 4,6,7,9