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

059-2025-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°059	Fecha: 11-03-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Un malware integrado en más de 280 aplicaciones falsas de Android utiliza OCR para robar contraseñas de criptocarteras		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Investigadores de ciberseguridad han identificado más de 280 aplicaciones fraudulentas en dispositivos Android que contienen un 'malware' diseñado para robar las credenciales de acceso a criptocarteras mediante una sofisticada tecnología de reconocimiento óptico de caracteres (OCR). Este 'malware', descubierto por el equipo de McAfee, se ha infiltrado en las aplicaciones a través de campañas de 'phishing', logrando obtener información confidencial de los usuarios.

2. DETALLES:

El OCR es una tecnología que convierte imágenes o documentos en texto, permitiendo que el 'malware' acceda a las claves nemotécnicas que los usuarios suelen almacenar mediante capturas de pantalla.

Estas claves son frases de doce palabras utilizadas para recuperar las criptocarteras en caso de pérdida. El 'malware' busca estas capturas en la galería de los dispositivos infectados, extrae las claves usando OCR y toma control de las carteras digitales.

Los ciberdelincuentes promueven estas aplicaciones a través de notificaciones urgentes que contienen enlaces maliciosos distribuidos en redes sociales. Estos enlaces redirigen a los usuarios a sitios web fraudulentos que imitan páginas legítimas y les solicitan descargar APKs infectadas.

Una vez instalada, la aplicación solicita permisos que permiten el acceso a información privada, como mensajes SMS, contactos e imágenes.

Además de robar las claves de las criptocarteras, el 'malware' puede funcionar en segundo plano, recibiendo y ejecutando instrucciones de un servidor remoto. Esto habilita al dispositivo infectado a participar en nuevas campañas de 'phishing'. Aunque la amenaza se ha identificado principalmente en Corea, se están tomando medidas para frenar su expansión.

A pesar de que este 'malware' no está muy extendido, McAfee advierte que su impacto es significativo debido a su capacidad para acceder a la lista de contactos del terminal y enviar mensajes engañosos.

Además, se ha señalado que el 'malware' ha evolucionado, comenzando como una falsa aplicación de préstamos o servicios gubernamentales, y adaptándose para explotar las emociones personales. Incluso ha llegado a imitar esquelas 'online'. Los expertos también sugieren que este ataque podría expandirse a dispositivos iOS en el futuro.

Monetización e impacto

El motivo principal detrás de estos ataques es el beneficio económico.

Los actores de amenazas explotan los datos robados drenando fondos de cuentas comprometidas, realizando transacciones no autorizadas o vendiendo las cuentas en mercados de la web oscura.

Además, el malware puede interceptar mensajes SMS, incluidas contraseñas de un solo uso utilizadas para la autenticación multifactorial, lo que permite a los atacantes eludir las medidas de seguridad.

El malware también puede realizar fraudes publicitarios ejecutándose silenciosamente en segundo plano para generar tráfico falso o suscribir a las víctimas a servicios premium sin su consentimiento.

La escala y la complejidad de esta operación indican un esfuerzo altamente coordinado para comprometer a los usuarios a nivel mundial, particularmente en el sudeste asiático.

3. RECOMENDACIONES:

- Descargar aplicaciones, asegurándose de que provengan de la tienda oficial Google Play Store y no de enlaces o sitios web sospechosos.
- Actualizar periódicamente el software de seguridad y estar atento a los permisos de las aplicaciones también pueden ayudar a mitigar el riesgo de este tipo de infecciones de malware.
- Utilizar software antivirus y antimalware.
- Utilizar contraseñas robustas y autenticación de dos factores.
- Configurar una política de seguridad en la red.

Fuente de Información:	• hxxps://gbhackers.com/playpraetor-malware-targets-android-users/ • hxxps://www.eltiempo.com/tecnosfera/novedades-tecnologia/un-malware-integrado-en-mas-de-280-aplicaciones-falsas-de-android-roba-contrasenas-de-criptocarteras-esta-es-la-tecnologia-que-utilizan-3380301

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°059	Fecha: 11-03-2025
		Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en SiPass Integrated AC5102 y SiPass Integrated ACC-AP de Siemens		
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:

Siemens AG ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo validación de entrada incorrecta que afecta a los sistemas de control SiPass Integrated AC5102 (ACC-G2) y SiPass Integrated ACC-AP de Siemens. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado realizar ataques de inyección de comandos.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-27494 de tipo validación de entrada incorrecta que afecta a Siemens SiPass Integrated AC5102 (ACC-G2) y SiPass Integrated ACC-AP, podría permitir a un atacante remoto no autenticado realizar ataques de inyección de comandos. La vulnerabilidad implica una limpieza de entrada incorrecta para el punto final de clave pública de la API REST. Esto podría permitir que un administrador remoto autenticado aumente los privilegios mediante la inyección de comandos arbitrarios que se ejecutan con privilegios de root.

Un administrador remoto autenticado con acceso de privilegios elevados puede aprovechar esta vulnerabilidad para ejecutar comandos arbitrarios con privilegios de nivel root. Esto podría provocar un compromiso total del sistema, incluido un posible acceso no autorizado, robo de datos, manipulación del sistema y la interrupción de la infraestructura crítica de control de acceso.

A. Productos afectados:

- SiPass Integrated AC5102 (ACC-G2), todas las versiones anteriores a V6.4.9.
- SiPass Integrated ACC-AP, todas las versiones anteriores a V6.4.9.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Restringir y monitorear el acceso a la API REST del administrador.
- Implementar la segmentación de la red para limitar la exposición.
- Utilizar mecanismos de autenticación fuertes.
- Aplicar el principio del mínimo privilegio para las cuentas de administrador.
- Monitorear los registros del sistema para detectar actividades sospechosas de la API REST.

Fuente de Información:	• hxxps://cert-portal.siemens.com/productcert/html/ssa-515903.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°059	Fecha: 11-03-2025 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de XSS en la interfaz gráfica de usuario de FortiADC de Fortinet		
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:

Fortinet, Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo secuencias de comandos entre sitios (XSS) que afecta a la interfaz gráfica de usuario de FortiADC. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante autenticado realizar un ataque XSS a través de solicitudes HTTP o HTTPS especialmente diseñadas.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2023-37933 de tipo secuencias de comandos entre sitios (XSS) que afecta a la interfaz gráfica de usuario de FortiADC, podría permitir a un atacante autenticado realizar un ataque XSS a través de solicitudes HTTP o HTTPS especialmente diseñadas.

Un atacante podría inyectar scripts maliciosos en páginas web, robar cookies de sesión de usuario, realizar acciones en nombre de la víctima, comprometer credenciales de usuario y redirigir a los usuarios a sitios web maliciosos.

A la fecha, no se tiene conocimiento de exploits públicos ni evidencia de explotación para esta vulnerabilidad. Si bien no hay ningún exploit de prueba de concepto público disponible, se recomienda a las organizaciones que actualicen su interfaz gráfica de usuario de FortiADC a las últimas versiones parcheadas para mitigar esta vulnerabilidad

A. Productos afectados:

- FortiADC, versión 7.4.0, 7.2.0 a 7.2.1 y anteriores a 7.1.3.

3. RECOMENDACIONES:

- Actualizar la interfaz gráfica de usuario de FortiADC a la última versión parcheada disponible que corrige esta vulnerabilidad.
- Implementar WAF para monitorear y filtrar el tráfico web, lo que puede ayudar a detectar y mitigar ataques XSS al bloquear solicitudes maliciosas.
- Implementar la segmentación de la red para limitar la propagación de posibles ataques. Adoptar una arquitectura de red de confianza cero (ZTNA) para controlar el acceso a aplicaciones y dispositivos, reduciendo el movimiento lateral.
- Verificar que toda la entrada del usuario esté validada y desinfectada para evitar que se inyecten scripts maliciosos en la aplicación.
- Implementar herramientas EDR para monitorear puntos finales en busca de actividad sospechosa y responder rápidamente a posibles vulnerabilidades.
- Realizar análisis de vulnerabilidad de rutina para identificar y priorizar los sistemas sin parches, garantizando que todas las vulnerabilidades conocidas se aborden rápidamente.
- Concientizar a los usuarios sobre los riesgos de los ataques XSS y cómo evitarlos, como no hacer clic en enlaces sospechosos o proporcionar información confidencial en respuesta a solicitudes no solicitadas.

Fuente de Información:	• hxxps://fortiguard.com/psirt/FG-IR-23-216

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°059	Fecha: 11-03-2025
		Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en Microsoft Management Console		
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:

Microsoft Corporation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo validación de entrada incorrecta que afecta a la herramienta Microsoft Management Console. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

Microsoft Management Console (MMC) es una herramienta de Microsoft Windows que permite a los usuarios y administradores de sistemas administrar y configurar el sistema.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-26633 de tipo validación de entrada incorrecta que afecta Microsoft Management Console. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y comprometer el sistema afectado.

La vulnerabilidad existe debido a una validación insuficiente de la información proporcionada por el usuario en Microsoft Management Console. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado y ejecute código arbitrario en el sistema de destino. Esta vulnerabilidad de día cero está siendo explotada activamente en la naturaleza.

A. Productos afectados:

- Windows: 10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.3194.
- Windows Server: 2008 R2 SP1 - 2025 10.0.26100.3194.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.

Fuente de Información:	• hxxp://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-26633 • hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633

Índice alfabético