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

086-2025-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°086	Fecha: 10-04-2025
		Página: 4 de 12

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Kellogg's sufre una brecha de datos tras un ciberataque a su proveedor Cleo		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

El gigante norteamericano de cereales conocido como Kellogg's ha sido víctima de una brecha de datos por un ciberataque a terceros. La compañía ha confirmado que la brecha afecta a sus servidores, alojados por la empresa Cleo, una plataforma reconocida que facilita la integración y el intercambio de datos entre sistemas empresariales. La intrusión no es reciente: ocurrió el 7 de diciembre de 2024, pero no fue descubierta hasta el 27 de febrero de este año, lo que genera serias dudas sobre los sistemas de monitoreo y detección de amenazas que la compañía y su proveedor tenían en funcionamiento.

2. DETALLES:

El grupo de ransomware CLOP publicó detalles sobre el incidente el 25 de febrero de 2025, aumentando la urgencia de que la empresa abordara la violación. Finalmente, el 4 de abril de 2025, WK Kellogg Co. presentó oficialmente un aviso de violación de datos ante las autoridades estatales y comenzó a notificar a las personas afectadas a través de una comunicación escrita.

Entre los datos robados se encuentran nombres y números de la Seguridad Social (SSN), lo que los convierte en material especialmente delicado para fraudes de identidad o suplantación digital.

El grupo CLOP empleó varias tácticas en su ataque:

- **Explotación de vulnerabilidades de día cero:** Aprovecharon vulnerabilidades sin parches en el software de Cleo para obtener acceso no autorizado a datos confidenciales. De hecho, fueron dos vulnerabilidades de día cero, identificadas como CVE-2024-50623 y CVE-2024-55956.
- **Exfiltración de datos:** Transfirieron de forma encubierta archivos de empleados que contenían información personal desde los servidores de Cleo.
- **Tácticas de ransomware:** Extorsionaron a la organización amenazando con filtrar los datos robados a menos que se pagara un rescate.

3. RECOMENDACIONES:

- Revisar con frecuencia los informes de crédito y movimientos bancarios.
- Activar los servicios de protección contra el robo de identidad ofrecidos por la empresa.
- Implementar el principio del privilegio mínimo para el acceso a información confidencial.
- Implementar políticas de contraseñas complejas y únicas.
- Activar el doble factor de autenticación en todo donde sea posible.
- Desarrollar planes de respuesta y recuperación ante incidentes que abarquen toda la cadena de suministro.
- Cifrar los datos en tránsito y en reposo.
- Denunciar inmediatamente cualquier uso no autorizado de sus datos.
- Capacitar a los empleados sobre las mejores prácticas de seguridad, incluyendo cómo identificar intentos de phishing y manejar información sensible.

Fuente de Información:	• hxxps://devel.group/blog/kelloggs-sufre-ciberataque-datos-filtrados-comprometen-informacion-sensible/ • hxxps://bitlifemedia.com/2025/04/kelloggs-sufre-una-brecha-de-datos-tras-un-ciberataque-a-su-proveedor-cleo/

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°086	Fecha: 10-04-2025
		Página: 5 de 12

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Estafa en WhatsApp quita el control de la aplicación y roba información confidencial		
Tipo de Ataque	Suplantación	Abreviatura	Suplantación
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G02
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

   Se ha alertado sobre una nueva modalidad de estafa en WhatsApp que podría hacer que los usuarios pierdan el control de sus cuentas.

2. **DETALLES:**

   Los ciberdelincuentes se hacen pasar por el equipo técnico de la plataforma y engañan a las víctimas, haciéndoles creer que están recibiendo asistencia para solucionar un supuesto error en la aplicación, “por ejemplo, que tu cámara no funciona”.

   Como parte del engaño, los estafadores realizan una videollamada y piden a la víctima que comparta la pantalla de su dispositivo. Si aceptas, el estafador verá todo lo que hagas en la pantalla.

   A continuación, el delincuente envía un código con el pretexto de continuar el proceso de reparación. En realidad, ese código permite al atacante acceder a la cuenta de WhatsApp de la víctima.

   De esta manera, el estafador puede suplantar su identidad y contactar a sus contactos para intentar nuevas estafas a través de la aplicación.

3. **RECOMENDACIONES:**

   - Contactar directamente con la aplicación WhatsApp a través de sus canales oficiales. El procedimiento consiste en abrir la aplicación, acceder al menú de "Ajustes", luego seleccionar la opción "Ayuda" y, dentro de esta sección, pulsar "Contáctanos".
     Una vez allí, el usuario debe describir cómo utiliza WhatsApp y proporcionar la información solicitada. Después de completar los campos requeridos, deberá tocar en la opción Enviar pregunta para establecer contacto con el servicio de atención.
     Adicionalmente, se puede consultar el Servicio de ayuda de WhatsApp a través de su sitio web, donde se ofrece información complementaria sobre diversas funciones y problemas comunes de la aplicación.
   - Aprender a identificar las estafas por WhatsApp reconociendo las señales como, por ejemplo, mensajes de números desconocidos o internacionales, solicitudes urgentes o inusuales, ofertas muy atractivas, suplantaciones de identidad de algún contacto tuyo, solicitudes de códigos de verificación, enlaces compartidos sospechosos, errores de ortografía o gramática, o videollamadas con solicitud de compartir pantalla. En esos casos, reportar el número a WhatsApp, bloquearlo de inmediato y alertar a otros contactos para evitar que también sean víctimas del engaño.
   - Hay que recordar que ningún representante oficial de WhatsApp pedirá un código de seis dígitos enviado por SMS.

Fuente de Información:	• hxxps://www.infobae.com/tecno/2025/04/05/nueva-estafa-en-whatsapp-quita-el-control-de-la-aplicacion-roba-datos-y-nunca-puedes-recuperarlos/

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°086	Fecha: 10-04-2025
		Página: 6 de 12

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Una falla en el Smart Hub de TP-Link expone las credenciales de Wi-Fi de los usuarios		
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:**

   Se ha descubierto una vulnerabilidad crítica en el Smart Hub de TP-Link, que podría exponer las credenciales de Wi-Fi de los usuarios a actores maliciosos.

2. **DETALLES:**

   Esta falla podría permitir a los atacantes obtener acceso no autorizado a información confidencial como las credenciales de Wi-Fi, lo que representa riesgos importantes para los usuarios afectados.

   La vulnerabilidad, identificada como CVE-2025-0072, afecta a los dispositivos Smart Hub de TP-Link.

   La explotación de esta falla podría permitir a los atacantes interceptar y hacer mal uso de estas credenciales, lo que provocaría más violaciones de seguridad dentro de la red del usuario.

   La falla existe debido a una validación de entrada insuficiente y al manejo inadecuado de las solicitudes de autenticación.

   Los atacantes pueden explotar esta vulnerabilidad enviando paquetes especialmente diseñados al dispositivo, eludiendo los protocolos de seguridad y obteniendo acceso a la información Wi-Fi almacenada.

   Una vez comprometidas las credenciales, los atacantes pueden infiltrarse en la red de la víctima y potencialmente acceder a otros dispositivos conectados y datos confidenciales.

   Productos afectados:

Nombre del producto	Número de modelo	Versión de firmware
Concentrador inteligente TP-Link	SH-TL001	Versiones anteriores a la 1.2
Puerta de enlace para casa inteligente TP-Link	SHG-TL002	Versiones anteriores a la 2.0

   Los expertos en seguridad advierten que esta vulnerabilidad podría ser explotada de forma remota, lo que la hace especialmente peligrosa para los usuarios que no hayan actualizado el firmware de sus dispositivos o implementado medidas de seguridad adicionales.

3. **RECOMENDACIONES:**

   - Actualizar sus dispositivos a la última versión de firmware disponible en el sitio web oficial de TP-Link.
   - Desconectar los dispositivos afectados de la red, en caso de que no se pueda actualizar su firmware rápidamente.
   - Utilizar contraseñas seguras para las redes Wi-Fi y habilitar protocolos de cifrado para ayudar a mitigar los riesgos.

Fuente de Información:	• hxxps://gbhackers.com/tp-link-smart-hub-flaw/#google_vignette

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°086	Fecha: 10-04-2025 Página: 7 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en dispositivos Siemens Industrial Edge		
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 autenticación débil que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir la autenticación y suplantar la identidad de usuarios legítimos a través de endpoints de API específicos cuando se utiliza la federación de identidades.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-54092 de tipo autenticación débil que afecta a múltiples de sus dispositivos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir la autenticación y suplantar la identidad de usuarios legítimos a través de endpoints de API específicos cuando se utiliza la federación de identidades.

Los dispositivos afectados no aplican correctamente la autenticación de usuario en puntos finales de API específicos cuando se utiliza la federación de identidades. Esto podría facilitar que un atacante remoto no autenticado eluda la autenticación y se haga pasar por un usuario legítimo.

Hasta el momento, no se tiene conocimiento de explotación pública dirigida específicamente a esta vulnerabilidad. Se recomienda implementar las medidas de mitigación recomendadas de forma proactiva.

A. Productos afectados:

- Siemens Industrial Edge Own Device (IEOD): todas las versiones anteriores a V1.21.1-1-a.
- Siemens Industrial Edge Virtual Device: todas las versiones anteriores a V1.21.1-1-a.
- Siemens SCALANCE LPE9413 (6GK5998-3GS01-2AC2): todas las versiones.
- Siemens SIMATIC IPC127E Industrial Edge Device: todas las versiones anteriores a V3.0.
- Siemens SIMATIC IPC227E Industrial Edge Device: todas las versiones anteriores a V3.0.
- Siemens SIMATIC IPC427E Industrial Edge Device: todas las versiones.
- Siemens SIMATIC IPC847E Industrial Edge Device: todas las versiones anteriores a V3.0.
- Siemens SIMATIC IPC BX-39A Industrial Edge Device: todas las versiones anteriores a V3.0.
- Siemens SIMATIC IPC BX-59A Industrial Edge Device: todas las versiones anteriores a V3.0.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de firmware disponible que abordan esta vulnerabilidad.
- Proteger el acceso a la red de los dispositivos con mecanismos adecuados.
- Configurar el entorno según sus directrices operativas de seguridad industrial y seguir las recomendaciones de los manuales de producto, para operar los dispositivos en un entorno de TI protegido.

Fuente de Información:	• hxxps://cert-portal.siemens.com/productcert/html/ssa-634640.html • hxxps://cert-portal.siemens.com/productcert/html/ssa-819629.html • hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-100-04

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°086	Fecha: 10-04-2025 Página: 8 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades en FortiAnalyzer y FortiManager 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 dos vulnerabilidades de severidad **ALTA** de tipo falta de autenticación para función crítica e inyección SQL en FortiAnalyzer y FortiManager. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado obtener acceso a información confidencial. Igualmente, un usuario remoto con privilegios puede ejecutar código o comandos no autorizados mediante solicitudes diseñadas a la aplicación afectada.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-35277 de tipo falta de autenticación para función crítica en FortiManager, podría permitir a un atacante remoto no autenticado obtener acceso a información confidencial. Un atacante tendría que enviar una solicitud especialmente diseñada a la aplicación afectada para explotar esta vulnerabilidad. La vulnerabilidad existe debido a la falta de autenticación para una función crítica. Un atacante remoto no autenticado puede extraer la configuración de todos los dispositivos administrados.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2024-35275 de tipo inyección SQL en FortiAnalyzer y FortiManager, podría permitir que un usuario privilegiado remoto ejecute código arbitrario. La vulnerabilidad existe debido a la neutralización incorrecta de elementos especiales utilizados en un comando SQL ('inyección SQL') en el demonio sdnproxy. Un usuario remoto con privilegios puede ejecutar código o comandos no autorizados mediante solicitudes diseñadas a la aplicación afectada para explotar esta vulnerabilidad.

A. Productos afectados:

- FortiAnalyzer: 7.4.0 - 7.4.3.
- FortiAnalyzer Cloud: 7.4.1 - 7.4.2.
- FortiManager: 6.4.0 - 7.4.2.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de firmware disponibles que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://www.fortiguard.com/psirt/FG-IR-24-135 • hxxps://fortiguard.fortinet.com/psirt/FG-IR-24-091

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°086	Fecha: 10-04-2025
		Página: 9 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ataque de suplantación de identidad en WhatsApp para escritorio		
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:**

Facebook, Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo representación errónea de información crítica en la interfaz de usuario (UI) que afecta a la aplicación para escritorio WhatsApp. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y realizar un ataque de suplantación de identidad.

2. **DETALLES:**

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-30401 de tipo representación errónea de información crítica en la interfaz de usuario (UI) que afecta a la aplicación para escritorio WhatsApp, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y realizar un ataque de suplantación de identidad.

La vulnerabilidad existe debido al procesamiento incorrecto de los archivos adjuntos dentro de la aplicación. La interfaz mostraba el tipo de archivo adjunto según su tipo MIME, pero seleccionaba el controlador de apertura según la extensión del archivo. Un atacante remoto puede engañar a la víctima para que abra un archivo adjunto especialmente diseñado y ejecutar código arbitrario en el sistema.

A. Productos afectados:

- WhatsApp para escritorio: 2.2017.6 - 24.2.76.

3. **RECOMENDACIÓN:**

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

Fuente de Información:	• hxxps://www.facebook.com/security/advisories/cve-2025-30401 • hxxps://www.whatsapp.com/security/advisories/2025/ • hxxps://cve.org/CVERecord?id=CVE-2025-30401

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°086	Fecha: 10-04-2025 Página: 10 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en productos de Gitlab		
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:

GitLab, Inc. ha publicado una vulnerabilidad de severidad **MEDIA** de tipo asignación de recursos sin límites ni limitaciones que afecta a GitLab Community Edition (CE) y Enterprise Edition (EE). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-1677 de tipo asignación de recursos sin límites ni limitaciones, podría permitir a un atacante remoto realizar un ataque de DoS inyectando cargas útiles de gran tamaño en las exportaciones de la canalización de CI.

La vulnerabilidad existe debido a una validación insuficiente de la entrada proporcionada por el usuario dentro de las canalizaciones de CI, que puede ser explotada por un usuario remoto autenticado a través de internet.

A. Productos afectados:

- GitLab CE: 0.1.5 anteriores a 17.10.3.
- GitLab EE: 6.2.0 anteriores a 17.10.3.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//about[.]gitlab[.]com/releases/2025/04/09/patch-release-gitlab-17-10-4-released/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°086	Fecha: 10-04-2025
		Página: 11 de 12

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en productos IBM		
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:**

IBM Corporation ha publicado una vulnerabilidad de severidad **MEDIA** de tipo asignación incorrecta de privilegios que afecta a IBM Guardium Data Protection. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto obtener acceso a información confidencial.

2. **DETALLES:**

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-25023 de tipo asignación de recursos sin límites ni limitaciones, podría permitir a un atacante remoto obtener acceso a información confidencial.

La vulnerabilidad existe debido a una asignación incorrecta de privilegios. Un atacante con privilegios puede obtener acceso no autorizado a información confidencial del sistema.

A. **Productos afectados:**

- IBM Security Guardium: anterior a la versión 11.0 hasta la 12.1.

3. **RECOMENDACIÓN:**

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

Fuente de Información:	• hxxps[:]//www[.]ibm[.]com/support/pages/node/7230467

Índice alfabético