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

104-2025-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°104	Fecha: 05-05-2025
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El ransomware Gunra y su impacto global		
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:

Recientemente ha surgido otro actor de ransomware que opera bajo el nombre de Gunra, apuntando a sistemas Windows, presuntamente cobrándose varias víctimas en los sectores de la salud, la electrónica, fabricación de bebidas, bienes raíces, productos farmacéuticos y manufactura.

2. DETALLES:

Gunra, derivado de Conti Ransomware y codificado en C/C++, filtra información empresarial confidencial antes de bloquear el sistema, agrega una extensión ".ENCRT" a los archivos cifrados y coloca una nota de rescate llamada "R3ADM3.txt" en los directorios afectados, afirmando que la única forma de recuperar los archivos es contactándolos para obtener una clave privada y una herramienta de descifrado.

Para aumentar la presión, el mensaje impone un plazo de cinco días, tras el cual los datos robados supuestamente se publicarán en la dark web si no se establece contacto.

Se indica a las víctimas que descarguen el navegador Tor, visiten un sitio .onion específico, se registren, inicien sesión e inicien la comunicación.

El ransomware Gunra emplea técnicas avanzadas de evasión y antianálisis para infectar sistemas operativos Windows, minimizando al mismo tiempo el riesgo de detección. Sus capacidades de evasión incluyen la ofuscación de actividades maliciosas, la evasión de sistemas de detección basados en reglas, métodos de cifrado robustos, exigencias de rescate y advertencias para publicar datos en foros clandestinos.

Tras la infección, enumera los procesos que se están ejecutando y recopila información del sistema mediante reconocimiento, elimina copias instantáneas a través del Instrumental de administración de Windows (WMI) desactivando así las funciones de restauración y copia de seguridad del sistema para garantizar que el cifrado sea irreversible sin ayuda externa

Sus capacidades anti-análisis incluyen el uso de la API IsDebuggerPresent, para evadir la detección, dificultar la ingeniería inversa y detectar depuradores como x64dbg y WinDbg, junto con la manipulación de procesos a través de las funciones GetCurrentProcess y TerminateProcess para la escalada de privilegios y la inyección de código malicioso en otros procesos y herramientas antimalware.

El ransomware emplea FindNextFileExW y funciones relacionadas para descubrir y cifrar archivos con extensiones como .docx, .pdf y .jpg, lo que garantiza un bloqueo completo de los datos. Utiliza FileNextFilew para continuar la enumeración de archivos, y FileClose pra liberar el identificador de FindFirstFileExW.

Su alineación con el marco MITRE ATT&CK revela tácticas que abarcan:

- Ejecución -> T1047: Instrumental de administración de Windows.
- Persistencia -> T1542: Bootkit.
- Escalada de privilegios -> T1055: Inyección de procesos y T1574: Carga lateral de DLL.
- Evasión de defensa -> T1027: Archivos ofuscados y T1564: Archivos y directorios ocultos.
- Acceso a credenciales -> T1539: Robo de cookies de sesión web y T1555: Credenciales de navegadores web.
- Descubrimiento -> T1082: Descubrimiento de información del sistema.
- Colección -> T1185: Secuestro de sesiones de navegadores.

- Mando y Control -> T1090: Proxy
- Impacto -> T1486: Cifrado de datos.

Indicadores de Compromiso:

Tipo de indicador:	**Valor:**
MD5	9a7c0adedc4c68760e49274700218507
SHA-256	854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd

3. RECOMENDACIONES:

- Realizar el bloqueo de los indicadores de compromiso listados.
- Implementar la supervisión de la actividad anormal de WMI (Instrumental de administración de Windows), especialmente relacionada con la eliminación de copias de sombra o la manipulación de servicios.
- Ejecutar la estrategia 3-2-1-1-0 de copias de seguridad, que consiste en realizar periódicamente tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube; además una de las copias esté disponible fuera de conexión, y cero copias sin verificar o con errores.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Invertir en soluciones de seguridad, como sistemas de detección y respuesta de endpoints (EDR), y software de detección y prevención de intrusiones (IDS/IPS), que utilicen inteligencia artificial y aprendizaje automático para la detección proactiva de amenazas, de tal manera que pueda identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- Habilitar la protección de archivos en tiempo real en los puntos finales para detectar la creación de nuevos archivos cifrados (con extensión .ENCRT) y evitar modificaciones de archivos por procesos no autorizados.
- Segmentar redes para restringir el movimiento lateral desde los dispositivos infectados.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de ransomware.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Desarrollar planes de respuesta y recuperación ante incidentes, que incluya promover la cooperación global en el intercambio de información sobre amenazas, y el fortalecimiento de capacidades de respuesta ante incidentes.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados. Estos programas pueden detectar y eliminar ransomware y otro software malicioso antes de que puedan cifrar sus archivos.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://www.cyfirma.com/research/gunra-ransomware-a-brief-analysis/ • hxxps://www.broadcom.com/support/security-center/protection-bulletin/gunra-ransomware

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°104	Fecha: 05-05-2025 Página: 6 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en IBM Business Automation Workflow para FreeType		
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 **ALTA** de tipo escritura fuera de límites que afecta a IBM Business Automation Workflow para FreeType. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y comprometer el sistema.

2. DETALLES:

FreeType es una biblioteca de software disponible gratuitamente para renderizar fuentes.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-27363 de tipo escritura fuera de límites que afecta a IBM Business Automation Workflow para FreeType, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y comprometer el sistema.

La vulnerabilidad existe debido a un error de límite al procesar entradas no confiables. Un atacante remoto puede pasar una fuente especialmente diseñada a la aplicación que usa una versión afectada de la biblioteca, activar una escritura fuera de límites y ejecutar código arbitrario en el sistema objetivo.

IBM indicó que existe una prueba de concepto y detalles técnicos disponibles para pruebas y validación.

A. Productos afectados:

- IBM Business Automation Workflow: 24.0.0, 24.0.0-IF001, 24.0.0-IF002, 24.0.0-IF003, 24.0.0-IF004, 24.0.1-IF001, 24.0.1.0.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad

Fuente de Información:	• hxxps://www.ibm.com/support/pages/node/7232436 • hxxps://github.com/zhuowei/CVE-2025-27363-proof-of-concept

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°104	Fecha: 05-05-2025 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica de inyección SQL en la biblioteca de abstracción de bases de datos PHP ADOdb		
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:

GitHub, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección SQL en ADOdb, una biblioteca de abstracción de bases de datos PHP. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar comandos SQL arbitrarios cuando el código que usa ADOdb se conecta a una base de datos PostgreSQL e invoca pg_insert_id() con datos proporcionados por el usuario.

2. DETALLES:

ADOdb es una biblioteca de clases de bases de datos PHP que proporciona abstracciones para realizar consultas y administrar bases de datos.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-46337 de tipo inyección SQL en ADOdb, una biblioteca de abstracción de bases de datos PHP, podría permitir a un atacante remoto no autenticado ejecutar comandos SQL arbitrarios en aplicaciones vulnerables. Los atacantes pueden obtener acceso no autorizado, manipular datos o comprometer completamente la base de datos.

La falla se encuentra en el pg_insert_id()método del controlador PostgreSQL, donde el escape incorrecto de un parámetro de consulta permite a los atacantes ejecutar sentencias SQL arbitrarias si se utiliza la entrada proporcionada por el usuario

La vulnerabilidad se activa cuando una entrada controlada por el usuario se pasa como parámetro $fieldname a la función pg_insert_id() sin la debida limpieza. Esto permite al atacante manipular la consulta SQL resultante y comprometer la base de datos subyacente.

Actualmente no hay ninguna prueba de concepto pública disponible, pero se ha confirmado que la vulnerabilidad es explotable.

A. Productos afectados:

- ADOdb, versiones anteriores a 5.22.9 (11107d6).
- Controladores PostgreSQL, incluidos postgres64, postgres7, postgres8 y postgres9.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://github.com/ADOdb/ADOdb/security/advisories/GHSA-8x27-jwjr-8545 • hxxps://github.com/ADOdb/ADOdb/issues/1070 • hxxps://xaliom.blogspot.com/2025/05/from-sast-to-cve-2025-46337.html • hxxps://github.com/ADOdb/ADOdb/commit/11107d6d6e5160b62e05dff8a3a2678cf0e3a426

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°104	Fecha: 05-05-2025
		Página: 8 de 10

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

Nvidia Corporation ha publicado una vulnerabilidad de severidad **ALTA** de tipo deserialización de datos no confiables que afecta a todas las plataformas Windows, Linux y macOS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante con acceso local al servidor TRTLLM ejecutar código arbitrario, divulgar información confidencial o manipular datos.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-23254 de tipo deserialización de datos no confiables, podría permitir a un atacante con acceso local al servidor TRTLLM ejecutar código arbitrario, divulgar información confidencial o manipular datos.

La falla se encuentra en el componente ejecutor de Python, específicamente en la gestión de la comunicación entre procesos (IPC), donde el módulo pickle de Python se utiliza para la serialización y deserialización. La validación incorrecta de este proceso de deserialización.

A. Productos afectados:

- NVIDIA TensorRT-LLM versiones anteriores a 0.18.2 (todos los SO).

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que abordan esta vulnerabilidad.

Fuente de Información:	• hxxps[:]//nvidia[.]custhelp[.]com/app/answers/detail/a_id/5648

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°104	Fecha: 05-05-2025 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en productos Zimbra		
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:

Zimbra Collaboration ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo falsificación de solicitud entre sitios (CSRF) que afecta al endpoint GraphQL (/service/extension/graphql) que carece de la validación de tokens CSRF adecuada. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante secuestrar sesiones autenticadas engañando a los usuarios conectados para que visiten sitios web o enlaces maliciosos, lo que podría provocar la apropiación de cuentas, el robo de datos y la escalada de privilegios en dominios completos.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-32354 de tipo falsificación de solicitud entre sitios (CSRF), podría permitir a un atacante secuestrar sesiones autenticadas engañando a los usuarios conectados para que visiten sitios web o enlaces maliciosos, lo que podría provocar la apropiación de cuentas, el robo de datos y la escalada de privilegios en dominios completos. La falla reside en el punto final GraphQL de Zimbra (/service/extension/graphql), que carece de validación de token CSRF.

A. Productos afectados:

- Zimbra Collaboration Suite (ZCS), versión 9.0 hasta la 10.1.3.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 10.1.4 o posterior que corrige esta vulnerabilidad.
- Aplicar la validación del token CSRF para las solicitudes GraphQL (por ejemplo, utilizando el encabezado X-Zimbra-CSRF-Token).
- Restringir el acceso al punto final GraphQL e implemente reglas de proxy inverso para validar los orígenes de las solicitudes.
- Habilitar la autenticación multifactor (MFA) para reducir los riesgos de secuestro de sesión.
- Supervisar los registros para detectar actividad inusual en GraphQL y educar a los usuarios sobre los riesgos de phishing.

Fuente de Información:	• hxxps[:]//wiki[.]zimbra[.]com/wiki/Centro_de_Seguridad; • hxxps[:]//wiki[.]zimbra[.]com/wiki/Zimbra_Responsible_Disclosure_Policy; • hxxps[:]//wiki[.]zimbra[.]com/wiki/Zimbra_Releases/10.1.4#Correcciones_de_Seguridad

Índice alfabético