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

139-2025-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°139	Fecha: 16-06-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	El ransomware Anubis agrega un limpiador para destruir archivos sin posibilidad de recuperación		
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:

Se ha descubierto una cepa emergente del ransomware Anubis que incorpora capacidades para cifrar archivos y borrarlos de forma permanente, un desarrollo que se ha descrito como una "rara amenaza dual".

Anubis (que no debe confundirse con el malware de Android del mismo nombre) es un Ransomware como Servicio (RaaS) relativamente nuevo que se observó por primera vez en diciembre de 2024, pero se volvió más activo a principios de año.

2. DETALLES:

Este ransomware no solo cifra los archivos de sus víctimas, sino que también cuenta con una funcionalidad de “wipe mode”, que requiere autenticación basada en clave para su emisión, y borra permanentemente los datos, haciendo imposible su recuperación incluso si se paga el rescate.

Además, existen versiones móviles de Anubis, especialmente dirigidas a dispositivos Android, que actúan como troyanos bancarios con múltiples capacidades de espionaje y robo de información.

El ransomware Anubis, ha afectado a organizaciones de los sectores salud, hotelero y de construcción en EE. UU., Canadá, Perú y Australia. Se distribuye a través de campañas de phishing y aprovecha accesos privilegiados para eliminar copias de seguridad (shadow copies), cifrar archivos y, en ciertos casos, borrarlos completamente.

En entornos de escritorio/servidores, realiza el cifrado de archivos y eliminación de backups locales, tiene la opción de borrado permanente (wipe), reduciendo archivos a 0 KB y manteniendo intactos los nombres y estructura de los archivos.

La víctima seguirá viendo todos los archivos en los directorios esperados, pero su contenido se destruirá irreversiblemente, lo que hará imposible la recuperación.

Los directorios importantes del sistema y del programa se excluyen de forma predeterminada para evitar que el sistema quede completamente inutilizable.

El ransomware elimina las instantáneas de volumen y finaliza los procesos y servicios que podrían interferir con el proceso de cifrado.

El sistema de cifrado utiliza ECIES (Elliptic Curve Integrated Encryption Scheme), y los investigadores notaron similitudes de implementación con EvilByte y el ransomware Prince.

A los archivos cifrados se les añade la extensión '.anubis', se coloca una nota de rescate HTML en los directorios afectados y el malware también intenta cambiar el fondo de pantalla del escritorio.

En entornos móviles (Android), realiza el robo de credenciales, archivos y datos bancarios mediante abuso de accesibilidad, intercepción de SMS, incluyendo códigos OTP de MFA, rastreo de ubicación por GPS, keylogging, grabación de audio y captura de pantallas, bloqueo del dispositivo, y exigencia de rescate para su desbloqueo.

Anubis admite varios comandos al iniciarse, incluidos elevación de privilegios, exclusión de directorios y rutas de destino para cifrado.

Indicadores de Compromiso

Nombre de detección	Rescate.Win64.NUBIAS.THDBIBE.go
SHA256	98a76aacbaa0401bac7738ff966d8e1b 0fe2d8599a266b111fdc932ce385c8ed

3. RECOMENDACIONES:

- Realizar el bloqueo de cualquier indicador de compromiso identificado asociado a algún ransomware.
- Implementar EDR y soluciones anti-ransomware con capacidades de detección de wipers, 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 red para evitar que las aplicaciones o los usuarios accedan a dominios maliciosos y otro contenido malicioso en Internet.
- 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.
- Promover la cooperación global en el intercambio de información sobre amenazas, el desarrollo de marcos regulatorios y el fortalecimiento de capacidades de respuesta ante incidentes.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Descargar sólo apps desde tiendas oficiales y validar su legitimidad.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de ransomware y auditar cuentas de usuario con privilegios administrativos.
- Utilizar soluciones de seguridad móvil.
- Habilitar la autenticación multifactor (MFA) para todos los servicios en la medida de lo posible, basado en tokens o aplicaciones seguras, no SMS.
- Desarrollar planes de respuesta ante incidentes que abarquen toda la cadena de suministro.
- Fortalecer sus políticas de gestión de dispositivos móviles.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Segmentar redes para restringir el movimiento lateral desde los dispositivos infectados.
- 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.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/anubis-ransomware-adds-wiper-to-destroy-files-beyond-recovery/ • hxxps://csirt.telconet.net/comunicacion/noticias-seguridad/nuevo-ransomware-anubis-combina-cifrado-y-borrado-de-archivos/ • hxxps://www.infobae.com/america/agencias/2025/06/16/el-ransomware-anubis-agrega-una-funcion-para-borrar-los-archivos-encriptados/ • hxxps://ciberprisma.org/2025/06/15/el-ransomware-anubis-agrega-una-nueva-estrategia-para-eliminar-archivos-sin-posibilidad-de-recuperacion/ • hxxps://thehackernews.com/2025/06/anubis-ransomware-encrypts-and-wipes.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°139	Fecha: 16-06-2025 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en la plataforma SailPoint IdentityIQ		
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:

SailPoint Technologies, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo control de acceso inadecuado que afecta a la plataforma de gestión de identidades y accesos (IAM) IdentityIQ. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la exposición de datos, posible ejecución de código y escalada de privilegios.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-10905 de tipo control de acceso inadecuado en SailPoint IdentityIQ, podría permitir a un atacante remoto no autenticado obtener acceso no autorizado a una funcionalidad que de otro modo estaría restringida. La vulnerabilidad existe debido a la falta de restricciones de acceso al contenido estático en el directorio de la aplicación IdentityIQ. Un atacante remoto puede acceder directamente a los archivos de la aplicación.

La vulnerabilidad permite el acceso HTTP/HTTPS no autorizado a contenido estático dentro del directorio de la aplicación IdentityIQ que debería estar protegido. Esto se debe al manejo inadecuado de los nombres de archivo que identifican recursos virtuales, lo que funciona como una falla de navegación de directorio. Los atacantes pueden explotar esta vulnerabilidad para acceder a archivos y directorios restringidos, incluidos archivos de configuración confidenciales, código de aplicación y datos de usuario, así como, omitir la autenticación, ejecutar código arbitrario o escalar privilegios dentro de la plataforma IAM.

A. Productos afectados:

- SailPoint IdentityIQ: 8,4 < 8,4p2, 8,3 < 8,3p5, 8,2 < 8,2p8, todas las versiones anteriores.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Restringir el acceso a la plataforma IAM a rangos de IP confiables.
- Aplicar los principios de mínimo privilegio.
- Implementar la autenticación multifactor (MFA).
- Supervisar y auditar el acceso a API y directorios para detectar actividades sospechosas.

Fuente de Información:	• hxxps://www.sailpoint.com/security-advisories/identityiq-improper-access-control-vulnerability-cve-2024-10905

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°139	Fecha: 16-06-2025 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el router D-Link DIR-632		
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:

D-Link Corporation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo restricción incorrecta de operaciones dentro de los límites de un búfer de memoria que afecta al router D-Link DIR-632. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado comprometer por completo el dispositivo afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-6121 de tipo restricción incorrecta de operaciones dentro de los límites de un búfer de memoria que afecta al router D-Link DIR-632 FW103B08, podría permitir a un atacante remoto no autenticado comprometer por completo el dispositivo afectado. Dado el vector de ataque basado en la red y su baja complejidad, esta vulnerabilidad puede explotarse fácilmente para tomar el control total del dispositivo.

La vulnerabilidad afecta a la función *get_pure_content* del componente *HTTP POST Request Handler*. La manipulación del argumento *Content-Length* provoca un desbordamiento del búfer en la pila. El ataque puede ejecutarse remotamente. El exploit se ha hecho público y puede utilizarse. Esta vulnerabilidad solo afecta a los productos que ya no reciben soporte del mantenedor.

A. Productos afectados:

- Router D-Link DIR-632, firmware FW103B08.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de firmware disponible que aborda esta vulnerabilidad.
- Aislar inmediatamente los dispositivos D-Link DIR-632 afectados con la versión de firmware FW103B08.
- Reemplazar los dispositivos no compatibles.
- Implementar la segmentación de red para restringir el acceso a dispositivos vulnerables.
- Utilizar firewalls de aplicaciones web (WAF) para filtrar potencialmente solicitudes HTTP POST maliciosas.
- Monitorear el tráfico de red para detectar posibles intentos de explotación.

Fuente de Información:	• hxxps://github.com/xiaobor123/vul-finds/tree/main/vul-find-dir632-dlink-get_pure_content • hxxps://github.com/xiaobor123/vul-finds/tree/main/vul-find-dir632-dlink-get_pure_content#poc

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°139	Fecha: 16-06-2025 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el software ASUS Armoury Crate		
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:

ASUSTeK Computer, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo condición de carrera de tiempo de verificación y tiempo de uso (TOCTOU) que afecta al software ASUS Armoury Crate, una utilidad utilizada para la administración y personalización de dispositivos ASUS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante local la omisión de autenticación, elevar privilegios y obtener acceso no autorizado a las funciones del sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-3464 de tipo condición de carrera de tiempo de verificación y tiempo de uso (TOCTOU) que afecta al software ASUS Armoury Crate, podría permitir a un atacante local la omisión de autenticación, elevar privilegios y obtener acceso no autorizado a las funciones del sistema.

Esta vulnerabilidad se debe a un problema de tiempo de uso y tiempo de comprobación, que podría provocar la omisión de la autenticación.

A. Productos afectados:

- ASUS Armoury Crate, desde la v5.9.9.0 hasta la v6.1.18.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://talosintelligence.com/vulnerability_reports/TALOS-2024-2150 • hxxps://www.asus.com/content/asus-product-security-advisory/ • hxxps://www.talosintelligence.com/vulnerability_reports/TALOS-2025-2150

Índice alfabético