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

125-2025-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°125	Fecha: 29-05-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	93.000 millones de cookies se han filtrado en la dark web		
Tipo de Ataque	Robo de información	Abreviatura	RobInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

Una investigación realizada por la compañía de ciberseguridad NordVPN ha puesto al descubierto que más de 93.000 millones de cookies se han filtrado en la dark web.

2. DETALLES:

Las cookies son pequeños archivos de texto que las páginas web almacenan en el navegador para recordar preferencias, datos de inicio de sesión y el comportamiento de navegación. Desempeñan un papel destacado para que la experiencia online sea más fluida: ayudan a que las páginas web se carguen antes, mantienen los carritos de compra llenos y permiten que los usuarios permanezcan conectados entre sesiones. Sin cookies, la comodidad y personalización de internet son muy limitadas.

El peligro: los ciberdelincuentes han aprendido a capturar cookies para secuestrar sesiones, robar identidades y eludir medidas de seguridad.

Cuando las cookies, que se utilizan como claves digitales para sesiones en línea y datos personales, quedan expuestas, se convierten en productos valiosos para los ciberdelincuentes. Esta infracción puede provocar el robo de información personal y financiera, el robo de identidad y transacciones no autorizadas.

Pero, ¿cómo se roba una cookie? Este proceso generalmente implica que un hacker obtenga información de sesión de un usuario sin su permiso. Esto puede suceder de diferentes maneras, como cuando un sitio web es vulnerable a ataques o cuando un usuario es engañado para revelar sus datos o accede a redes WiFi no seguras.

Los hackers también se valen de malware para robar las cookies de usuarios que no saben lo que está pasando. En nuestro estudio, los investigadores descubrieron que casi todos los datos terminaron en la dark web después de lanzar troyanos y ataques keyloggers. Estas categorías de malware están diseñadas específicamente para recopilar datos de inicio de sesión, cookies, contraseñas guardadas del navegador y monederos de criptomonedas. Estas son algunas de las herramientas más comunes detrás de las cookies web robadas en nuestra investigación:

- **Redline** es uno de los keyloggers y ladrones de información más utilizados, que se anuncia como malware como servicio. Redline Stealer es responsable de la mayor parte de las cookies robadas en nuestro conjunto de datos: casi 42.000 millones de cookies. Sin embargo, solo el 6,2% seguían activas, lo que significa que la vida útil de los datos robados es relativamente corta.
- **Vidar** también es un malware como servicio con configuraciones específicas diseñadas para atacar tipos concretos de datos. Recopiló alrededor de 10.500 millones de cookies, de las cuales el 7,2% seguían siendo válidas.
- **LummaC2** es un ladrón ofrecido como servicio a los ciberdelincuentes. Es más reciente pero su uso está creciendo rápidamente. Fue responsable de más de 8.800 millones de cookies robadas, con un 6,5% aún activo.
- **CryptBot** es un infostealer dirigido principalmente a sistemas operativos Windows. Aunque solo contabilizó 1.400 millones de cookies, el 83,4% de ellas seguían activas, lo que convierte a CryptBot en el malware más eficaz de nuestra lista.

Estas herramientas de malware son fáciles de usar y están ampliamente disponibles, lo que las hace accesibles a casi todo el mundo. A menudo se ocultan en software pirata o en descargas aparentemente inofensivas. Una vez instalados, escanean el almacenamiento de cookies del navegador y envían todo a un servidor de comando y control. Desde allí, los datos pueden aparecer en la dark web, a veces en cuestión de minutos.

En cuanto a las plataformas, como era de esperar, dominan los grandes nombres. Las cookies asociadas a los servicios de Google constituyeron la mayor parte del conjunto de datos: más de 4.500 millones de cookies vinculadas a Gmail, Google Drive y otros servicios de Google. YouTube y Microsoft representaron cada uno más de 1.000 millones de cookies.

Las plataformas más populares son objetivos apetecibles porque se puede obtener más información de ellas. Además, las cuentas de Google y Microsoft se utilizan a menudo para la autenticación multifactor. Robar una cookie de sesión de Google o Microsoft podría dar a los ciberdelincuentes acceso al correo electrónico, archivos, calendarios e incluso cuentas vinculadas, sin necesidad de adivinar contraseñas o activar la autenticación de dos factores.

"Cuando se filtra esta información, puede usarse no solo para ataques dirigidos sino también para publicidad invasiva y la creación de perfiles detallados de los comportamientos en línea de las personas, lo que infringe la privacidad y potencialmente conduce a censura o manipulación", comenta Marijus Briedis, director de tecnología de NordVPN.

Cuando las cookies, que se utilizan como claves digitales para sesiones en línea y datos personales, quedan expuestas, se convierten en productos valiosos para los ciberdelincuentes. Esta infracción puede provocar el robo de información personal y financiera, el robo de identidad y transacciones no autorizadas.

3. RECOMENDACIONES:

- Vigilar tu actividad online para evitar los riesgos derivados de filtraciones de información y malware.
- Usar contraseñas fuertes y únicas para cada cuenta.
- Activar la autenticación multifactor (MFA) siempre que sea posible.
- Tener cuidado al compartir información personal y evitar pulsar enlaces sospechosos o descargar archivos desconocidos.
- Eliminar con frecuencia los datos guardados en el navegador para proteger tu seguridad. Las sesiones activas pueden mantenerse incluso después de cerrar el navegador. Borrar estos datos reduce la posibilidad de accesos no autorizados.
- Revisar siempre los ajustes de privacidad de tus cuentas online para compartir información solo con servicios de confianza.
- Borrar de vez en cuando las cookies de tu navegador. Con esto al final consigues minimizar la cantidad de información que podría filtrarse o robarse.
- Mantener actualizado su sistema operativo, navegador y cualquier software instalado con los últimos parches y actualizaciones de seguridad. Muchos ciberataques aprovechan vulnerabilidades que ya han sido parcheadas en las últimas versiones del software.
- Elegir una VPN confiable para cambiar tu dirección IP y cifrar el tráfico de navegación, ya que hará más difícil que las cookies te rastreen en diferentes sitios.
- Educar a los empleados sobre las amenazas de correo electrónico malicioso y cómo identificarlo.

Fuente de Información:	• hxxps://www.escudodigital.com/ciberseguridad/93000-millones-cookies-se-han-filtrado-en-dark-web_63544_102.html • hxxps://nordvpn.com/es/blog/investigacion-cuantas-cookies-se-roban/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°125	Fecha: 29-05-2025 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Netwrix Directory Manager		
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 publicado una vulnerabilidad de severidad **CRÍTICA** de tipo uso de credenciales codificadas que afecta a Netwrix Directory Manager (anteriormente Imanami GroupID). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado el robo de datos, control y manipulación del sistema y la interrupción del servicio debido a un posible acceso no autorizado debido a la contraseña incorporada.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-48748 de tipo uso de credenciales codificadas que afecta a Netwrix Directory Manager, podría permitir a un atacante remoto no autenticado obtener el control total del sistema, robo de datos, manipulación del sistema y la interrupción del servicio. Esta falla de seguridad implica la presencia de una credencial estática e incrustada que podría ser fácilmente descubierta y explotada por atacantes.

El problema es una vulnerabilidad de contraseña de código duro, lo que significa que el software contiene una contraseña incrustada en su código que los atacantes podrían explotar para obtener acceso no autorizado o una escalada de privilegios.

Un atacante podría obtener acceso no autorizado al sistema Netwrix Directory Manager sin necesidad de interacción del usuario. Esta vulnerabilidad permite la vulneración total del sistema, con graves consecuencias para la confidencialidad, la integridad y la disponibilidad. Los riesgos potenciales incluyen la toma de control total del sistema, el robo de datos, la manipulación del sistema y la interrupción del servicio.

No hay evidencia de que exista una prueba de concepto pública. Actualmente, no hay evidencia de explotación.

A. Productos afectados:

- Netwrix Directory Manager, hasta la versión v.10.0.7784.0.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Aislar inmediatamente los sistemas afectados.
- Deshabilitar o restringir el acceso a la red a las instancias vulnerables de Netwrix Directory Manager.
- Aplicar las actualizaciones proporcionadas por el proveedor tan pronto como estén disponibles.
- Realizar una auditoría de seguridad integral para garantizar que no se haya producido ningún acceso no autorizado.
- Implementar credenciales sólidas y únicas y evitar las contraseñas codificadas en cualquier software.

Fuente de Información:	• hxxps://community.netwrix.com/t/adv-2025-013-hard-coded-password-in-netwrix-directory-manager-formerly-imanami-groupid-v10-and-earlier/13945

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°125	Fecha: 29-05-2025 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en IBM Tivoli Monitoring		
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 **CRÍTICA** de tipo validación incorrecta del índice, la posición o el desplazamiento especificados en la entrada que afecta a IBM Tivoli Monitoring. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario con privilegios completos del sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-3357 de tipo validación incorrecta del índice, la posición o el desplazamiento especificados en la entrada que afecta a IBM Tivoli Monitoring, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario debido a una validación incorrecta de un valor de índice de una matriz asignada dinámicamente.

No hay evidencia de que exista una prueba de concepto pública. Actualmente, no hay evidencia de explotación.

A. Productos afectados:

- IBM Tivoli Monitoring 6.3.0.7 a 6.3.0.7 Service Pack 19.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Aislar inmediatamente las instancias de Tivoli Monitoring afectadas.
- Aplicar los parches proporcionados por el proveedor tan pronto como estén disponibles.
- Implementar la segmentación de la red para restringir el acceso al sistema de monitoreo.
- Monitorear cualquier actividad inusual en la red o el sistema.
- Realizar una auditoría de seguridad integral del entorno.

Fuente de Información:	• hxxps://www.ibm.com/support/pages/node/7234923

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°125	Fecha: 29-05-2025 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Exploit para la inyección de comandos del sistema operativo en RT-AX55		
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 publicado una vulnerabilidad de severidad **ALTA** de tipo inyección de comandos del sistema operativo que afecta a los routers RT-AX55 de ASUS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar comandos de shell arbitrarios en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2023-39780 de tipo inyección de comandos del sistema operativo en enrutadores RT-AX55, podría permitir a un atacante remoto no autenticado ejecutar comandos de shell arbitrarios en el sistema de destino. Requiere autenticación; los atacantes manipulan los campos de entrada para ejecutar comandos arbitrarios del sistema.

La vulnerabilidad existe debido a una validación de entrada incorrecta en el parámetro "qos_bw_rulelist" de /start_apply.htm. Un usuario remoto puede pasar datos especialmente diseñados a la aplicación y ejecutar comandos arbitrarios del sistema operativo en el sistema objetivo. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

En mayo de 2025, se confirmó que más de 9000 enrutadores ASUS RT-AX55 estaban comprometidos en todo el mundo. Los atacantes utilizan técnicas sigilosas para evadir la detección, sin dejar malware, pero deshabilitando registros y utilizando funciones legítimas del enrutador para la persistencia. Los enrutadores comprometidos pueden estar integrados en redes de amenazas persistentes avanzadas (APT) o botnets

A. Productos afectados:

- ASUS RT-AX55: 3.0.0.4.386.51598.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de firmware disponible que aborda esta vulnerabilidad. ASUS ha lanzado actualizaciones de firmware que corrigen CVE-2023-39780 y otras vulnerabilidades de omisión de autenticación relacionadas.
- Realizar una revisión manual y eliminar las claves y configuraciones SSH no autorizadas, en caso se sospeche de algún compromiso.
- Realizar un restablecimiento de fábrica y rotar todas las credenciales de autenticación (contraseñas y claves SSH) para eliminar por completo las puertas traseras.

Fuente de Información:	• hxxps://github.com/D2y6p/CVE/blob/main/asus/CVE-2023-39780/1/EN.md • hxxps://github.com/D2y6p/CVE/blob/main/asus/CVE-2023-39780/2/EN.md • hxxps://github.com/D2y6p/CVE/blob/main/asus/CVE-2023-39780/3/EN.md • hxxps://github.com/D2y6p/CVE/blob/main/asus/CVE-2023-39780/4/EN.md • hxxps://github.com/D2y6p/CVE/blob/main/asus/CVE-2023-39780/5/EN.md • hxxps://github.com/D2y6p/CVE/blob/main/asus/CVE-2023-39780/6/EN.md

Índice alfabético