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

133-2025-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

Los piratas informáticos utilizan llamadas falsas de soporte técnico para vulnerar los sistemas corporativos y de Google . 4
Vulnerabilidad de severidad crítica en dispositivos TBK DVR-4104 y DVR-4216 de Visión TBK 5
Vulnerabilidad de ejecución remota de código en QNAP QES 6
Vulnerabilidad de severidad crítica en el software web ManageEngine Exchange Reporter Plus 7
Índice alfabético 8

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°133	Fecha: 09-06-2025
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Los piratas informáticos utilizan llamadas falsas de soporte técnico para vulnerar los sistemas corporativos y de Google		
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:**

Un grupo de piratas informáticos con motivaciones económicas, conocido como UNC6040, está utilizando una táctica simple pero efectiva para violar entornos empresariales: levantar el teléfono y hacerse pasar por soporte informático usando el phishing de voz (Vishing).

2. **DETALLES:**

La UNC6040 no se basa en exploits ni vulnerabilidades de seguridad. En cambio, se basa en errores humanos. Los atacantes llaman a los empleados y les explican cómo aprobar una aplicación conectada dentro de Salesforce. Pero no se trata de una aplicación cualquiera, sino que suele ser una versión modificada de la herramienta legítima Data Loader de Salesforce.

Con este acceso, los atacantes pueden consultar y extraer grandes cantidades de datos de la organización objetivo. En algunos casos, disfrazan la herramienta como "My Ticket Portal", un nombre que se ajusta al tema de soporte de TI de la estafa.

Una vez concedido el acceso, UNC6040 extrae los datos por etapas. A veces, comienzan con datos pequeños para evitar la detección, utilizando consultas de prueba y lotes limitados. Si el sondeo inicial pasa desapercibido, amplían la operación y comienzan una exfiltración de gran volumen.

Curiosamente, el robo de datos no siempre conlleva demandas inmediatas. En varios incidentes, transcurrieron meses antes de que las víctimas recibieran mensajes de extorsión. En dichos mensajes, los atacantes afirmaban estar asociados con el conocido grupo de hackers ShinyHunters, una medida probablemente destinada a presionar a las víctimas para que pagaran. Este enfoque tardío sugiere que UNC6040 podría estar trabajando con otros actores especializados en monetizar datos robados. Ya sea que vendan el acceso o entreguen los datos para ataques posteriores, la larga pausa dificulta la detección y respuesta a incidentes para los equipos de seguridad.

Aunque el objetivo principal es Salesforce, las ambiciones del grupo no terminan ahí. Una vez obtenidas las credenciales, se ha observado que UNC6040 se mueve lateralmente a través de los sistemas corporativos, atacando plataformas como Okta y Microsoft 365. Este acceso más amplio les permite recopilar datos valiosos adicionales, consolidar su presencia y generar influencia para futuros intentos de extorsión.

3. **RECOMENDACIONES:**

- 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.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de malware y auditar cuentas de usuario con privilegios administrativos.
- Restringir el acceso no autorizado a VPN o aplicaciones a rangos de IP de confianza
- Habilitar la autenticación multifactor (MFA) para todos los servicios en la medida de lo posible.
- Educar a los usuarios sobre cómo reconocer las amenazas de ingeniería social.

Fuente de Información:	• hxxps://hackread.com/hackers-fake-it-support-calls-breach-systems-google/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°133	Fecha: 09-06-2025
		Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en dispositivos TBK DVR-4104 y DVR-4216 de Visión TBK		
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:

Visión TBK ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección de comandos del sistema operativo que afecta a los dispositivos de grabación de vídeo digital TBK DVR-4104 y DVR-4216, explotada activamente por botnets como Mirai. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar comandos de shell arbitrarios del sistema operativo en el sistema objetivo.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-3721 de tipo inyección de comandos del sistema operativo que afecta a los dispositivos TBK DVR-4104 y DVR-4216, podría permitir a un atacante remoto no autenticado ejecutar comandos arbitrarios con los privilegios del proceso DVR, lo que podría provocar la violación total del dispositivo, la exfiltración de datos o su uso en operaciones de botnets.

La vulnerabilidad existe debido a una validación de entrada incorrecta en el manejo incorrecto del argumento mdb o mdc en /device.rsp?opt=sys&cmd=___S_O_S_T_R_E_A_MAX___.

Un atacante remoto no autenticado puede enviar una solicitud HTTP POST especialmente diseñada al dispositivo afectado 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.

Exploit público, explotado activamente en la naturaleza (variante de la botnet Mirai).

A. Productos afectados:

- TBK DVR4104: Todas las versiones.

B. Indicadores de compromiso (IoC):

- Hash: 011a406e89e603e93640b10325ebbdc8.
- Hash:24fd043f9175680d0c061b28a2801dfc.
- Hash:29b83f0aae7ed38d27ea37d26f3c9117.
- Hash:2e9920b21df472b4dd1e8db4863720bf.
- Nombres de detección de malware: HEUR:Backdoor.Linux.Mirai, HEUR:Backdoor.Linux.Gafgyt.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de firmware disponible que abordan esta vulnerabilidad.
- Aislar los dispositivos DVR en un segmento de red separado y restrinja el acceso tanto como sea posible.
- Implementar un firewall de aplicaciones web (WAF) para bloquear solicitudes maliciosas dirigidas al punto final vulnerable.
- Implementar la validación de entrada y la desinfección de los parámetros afectados.
- Monitorear actividades de red inusuales, especialmente conexiones salientes o descargas desde los dispositivos DVR.
- Considerar restablecerlo de fábrica, si acaso se cree que un dispositivo está comprometido después de aplicar el parche.

Fuente de Información:	• hxxps://github.com/netsecfish/tbk_dvr_command_injection • hxxps://vuldb.com/?ctiid.260573 • hxxps://vuldb.com/?id.260573 • hxxps://vuldb.com/?submit.314969

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°133	Fecha: 09-06-2025 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en QNAP QES		
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:

QNAP Systems, Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo condición de carrera que afecta al sistema operativo QNAP QES (QNAP Enterprise Storage). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y comprometer el sistema.

2. DETALLES:

QNAP QES (QNAP Enterprise Storage) es un sistema operativo de nivel empresarial diseñado para las soluciones NAS (almacenamiento conectado a red) de alta gama de QNAP, particularmente aquellas dirigidas al almacenamiento a gran escala, la virtualización y las aplicaciones comerciales de misión crítica.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-6387 de tipo condición de carrera que afecta al sistema operativo QNAP ES, podría permitir a un atacante remoto no autenticado ejecutar código arbitrario y comprometer el sistema.

La vulnerabilidad existe debido a una condición de carrera en la versión portátil de sshd. Un atacante remoto no autenticado puede enviar una serie de solicitudes para activar una condición de carrera y ejecutar código arbitrario en el sistema.

A. Productos afectados:

- QNAP QES: versiones anteriores a 2.2.1 20250304.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.qnap.com/en/security-advisory/qsa-25-13

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°133	Fecha: 09-06-2025 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el software web ManageEngine Exchange Reporter Plus		
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:

ManageEngine ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo carga sin restricciones de archivos de tipo peligroso que afecta al software web ManageEngine Exchange Reporter Plus. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución remota de código en el módulo de búsqueda de contenido.

2. DETALLES:

ManageEngine Exchange Reporter Plus es un software web integral de generación de informes, auditoría y supervisión, diseñado para entornos Microsoft Exchange, incluyendo Exchange Server, Exchange Online y Skype Empresarial.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-3835 de tipo carga sin restricciones de archivos de tipo peligroso que afecta al software Zoho ManageEngine Exchange Reporter Plus, podría permitir a un atacante remoto no autenticado la ejecución remota de código en el módulo de búsqueda de contenido. La vulnerabilidad requiere la interacción del usuario, pero puede activarse a través de una red con baja complejidad.

La vulnerabilidad se encuentra en el módulo de búsqueda de contenido y permite a los atacantes ejecutar comandos arbitrarios en el servidor objetivo, lo que podría comprometer la integridad del sistema.

A la fecha no se tiene conocimiento de algún exploits público que explote esta vulnerabilidad.

A. Productos afectados:

- ManageEngine Exchange Reporter Plus versiones anteriores a 5722.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Restringir el acceso de red al módulo de búsqueda de contenido.
- Implementar controles de acceso estrictos y monitorear actividades sospechosas.

Fuente de Información:	• hxxps://www.manageengine.com/products/exchange-reports/advisory/CVE-2025-3835.html

Índice alfabético

Explotación de vulnerabilidades conocidas 5, 6, 7
Suplantación 4