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

175-2024-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°175	Fecha: 30-07-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La estafa de phishing de OneDrive engaña a los usuarios para que ejecuten un script malicioso de PowerShell		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Las estafas de phishing continúan evolucionando y convirtiéndose en una amenaza cada vez más sofisticada para los usuarios de servicios en línea. Recientemente, se ha descubierto una nueva táctica que utiliza OneDrive como cebo, engañando a los usuarios para que ejecuten un script malicioso de PowerShell. Esta técnica no solo pone en riesgo la seguridad de tus datos, sino que también puede comprometer toda tu red.

2. DETALLES:

"Esta campaña se basa en gran medida en tácticas de ingeniería social para engañar a los usuarios para que ejecuten un script de PowerShell, comprometiendo así sus sistemas", dijo el investigador de seguridad de Trellix, Rafael Peña.

Denominada "OneDrive Pastejacking", la campaña inicia con un correo electrónico que contiene un archivo HTML adjunto. Al abrirlo, el archivo muestra una imagen que imita una página oficial de OneDrive y presenta un mensaje de error que afirma: "Error al conectarse al servicio en la nube 'OneDrive'. Para corregir el error, debe actualizar la caché DNS manualmente".

El mensaje ofrece dos opciones: "Cómo solucionarlo" y "Detalles". La opción de "Detalles" redirige a los usuarios a una página legítima de Microsoft Learn, donde se explican problemas comunes de DNS, lo que añade una capa de legitimidad al engaño. Sin embargo, al seleccionar "Cómo solucionarlo", los usuarios son guiados a realizar una serie de pasos que incluyen presionar "Tecla Windows + X" para abrir el menú Enlace rápido, iniciar la terminal de PowerShell, y pegar un comando codificado en Base64, que supuestamente resolverá el problema.

"El comando primero ejecuta ipconfig /flushdns, luego crea una carpeta en la unidad C: llamada 'downloads'", explicó Peña. "A continuación, descarga un archivo en esta ubicación, le cambia el nombre, extrae su contenido ('script.a3x' y 'AutoIt3.exe') y ejecuta script.a3x utilizando AutoIt3.exe", un programa que facilita la automatización de tareas en Windows.

En realidad, este comando ejecuta un script malicioso que puede comprometer la seguridad del sistema del usuario, permitiendo a los atacantes acceder a información sensible o controlar remotamente el equipo infectado. Este tipo de ataques, que explotan la confianza del usuario en servicios legítimos y su desconocimiento técnico, representan una amenaza significativa para la seguridad cibernética.

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos o no solicitados, ni descargar adjuntos de correos desconocidos.
- Utilizar software de seguridad. Proteger sus dispositivos con software antivirus actualizado, que pueda ayudar a detectar y bloquear descargas y sitios maliciosos, así como también habilitar la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.
- Descargar aplicaciones exclusivamente de fuentes oficiales.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://thehackernews.com/2024/07/onedrive-phishing-scam-tricks-users.html • hxxps://blog.tecnetone.com/phishing-en-onedrive-enga%C3%B1a-a-usuarios-para-ejecutar-script-powershell

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°175		Fecha: 30-07-2024
			Página: 5 de 8
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en Dell NetWorker Virtual Edition y Dell NetWorker Management Console		
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 reportado múltiples vulnerabilidades de severidad **ALTA** de tipo divulgación de información, desbordamiento de enteros, permisos, privilegios y controles de acceso, gestión inadecuada de privilegios e inyección CRLF que afecta a Dell NetWorker Virtual Edition y Dell NetWorker Management Console. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto inyectar datos arbitrarios en la respuesta del servidor, ejecutar código arbitrario, aumentar privilegios dentro de la base de datos, realizar un ataque de denegación de servicio (DoS) y obtener acceso a información confidencial.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-5869 de tipo desbordamiento de enteros, podría permitir a un usuario remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un desbordamiento de números enteros en la modificación de una matriz. Un usuario remoto puede pasar datos especialmente diseñados a la aplicación, provocar un desbordamiento de números enteros y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-0985 de tipo gestión inadecuada de privilegios, podría permitir a un usuario remoto aumentar privilegios dentro de la base de datos. La vulnerabilidad existe debido a una pérdida tardía de privilegios en REFRESH MATERIALIZED VIEW CONCURRENTLY. Un usuario remoto que es un creador de objetos puede ejecutar funciones SQL arbitrarias como emisor del comando.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2020-26137 de tipo inyección CRLF, podría permitir a un atacante remoto inyectar datos arbitrarios en la respuesta del servidor. La vulnerabilidad existe debido a una validación insuficiente de los datos proporcionados por el atacante que se pasan a través del parámetro "método". Un atacante remoto autenticado puede pasar datos especialmente diseñados a la aplicación que contengan caracteres CR-LF y modificar el comportamiento de la aplicación.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-45803 de tipo divulgación de información, podría permitir a un atacante remoto obtener acceso a información potencialmente confidencial. La vulnerabilidad existe debido a que urllib3 no elimina el cuerpo de la solicitud HTTP al redirigir la respuesta HTTP utilizando los códigos de estado 301, 302 o 303, después de que se haya cambiado el método de la solicitud de uno que pueda aceptar un cuerpo de solicitud (por ejemplo, de POST a GET). Un atacante remoto puede obtener acceso a información potencialmente confidencial.

Las vulnerabilidades de severidad baja asignadas por MITRE son: CVE-2023-5868, CVE-2023-5870 y CVE-2023-43804.

A. Productos afectados:

- Dell NetWorker Virtual Edition: antes de la versión 19.11.
- Consola de administración de NetWorker (NMC): anterior a la versión 19.11.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://www.dell.com/support/kbdoc/nl-nl/000226582/dsa-2024-012-security-update-for-dell-networker-virtual-edition-networker-management-console-multiple-component-vulnerabilities

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°175	Fecha: 30-07-2024 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Actualización de Red Hat Enterprise Linux 9 para openssh		
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 reportado una vulnerabilidad de severidad **ALTA** de tipo condición de carrera que afecta a Red Hat Enterprise Linux 9 para openssh. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario y comprometer el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-6409 de tipo condición de carrera que afecta Red Hat Enterprise Linux 9 para openssh, podría permitir a un atacante remoto comprometer el sistema afectado. La vulnerabilidad existe debido a una condición de carrera en la versión portátil de sshd al manejar señales. Si un atacante remoto no se autentica dentro de un período de tiempo determinado, se llama al controlador SIGALRM de sshd de forma asincrónica. Un atacante remoto no autenticado puede enviar una serie de solicitudes para activar una condición de carrera y ejecutar código arbitrario como un usuario sin privilegios que ejecuta el servidor sshd en el sistema.

A. Productos afectados:

- Red Hat Enterprise Linux Server para Power LE: servicios de actualización para soluciones SAP: 9.0.
- openssh (paquete Red Hat): anterior a 8.7p1-12.el9_0.3.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://access.redhat.com/errata/RHSA-2024:4910 • hxxps://cve.org/CVERecord?id=CVE-2024-6409

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°175	Fecha: 30-07-2024
		Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código por desbordamiento de búfer basado en pila en el kernel de Linux ksmbd		
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 reportado una vulnerabilidad de severidad **CRÍTICA** de tipo desbordamiento de búfer basado en pila en el kernel de Linux ksmbd. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remotos ejecutar código arbitrario en las instalaciones afectadas del kernel de Linux.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2023-52755 de tipo desbordamiento de búfer basado en pila en el kernel de Linux ksmbd, podría permitir a un atacante remoto ejecutar código arbitrario en las instalaciones afectadas del kernel de Linux. Es posible que se requiera o no autenticación para explotar esta vulnerabilidad, según la configuración. Además, solo los sistemas con ksmbd habilitado son vulnerables.

La vulnerabilidad existe en el procesamiento de los atributos de ACL. El problema es el resultado de la falta de una validación adecuada de la longitud de los datos proporcionados por el usuario antes de copiarlos a un búfer basado en montón de longitud fija. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del núcleo.

A. Productos afectados:

Las siguientes versiones del Kernel de Linux que se ven afectados son:

- Afectado desde 1da177e4c3f4 antes de 8387c94d73ec.
- Afectado desde 1da177e4c3f4 antes de 09d9d8b40a33.
- Afectado desde 1da177e4c3f4 hasta 712e01f32e57.
- Afectado desde 1da177e4c3f4 antes de eebff19acaa3.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://lore.kernel.org/all/20231124172008.838629931@linuxfoundation.org/ • hxxps://www.cve.org/CVERecord?id=CVE-2023-52755 • hxxps://git.kernel.org/stable/c/aaf0a07d60887d6c36fc46a24de0083744f07819 • hxxps://git.kernel.org/stable/c/8387c94d73ec66eb597c7a23a8d9eadf64bfbafa

Índice alfabético