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

# 170-2024-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°170 | Fecha: 22-07-2024 |
|---|---|---|
| | | Página: 4 de 9 |

| | | | |
|---|---|---|---|
| Componente que reporta | CENTRO NACIONAL DE SEGURIDAD DIGITAL | | |
| Nombre de la alerta | Descubierto un zero-day en Telegram que permite enviar APKs maliciosos disfrazados de vídeos | | |
| 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:

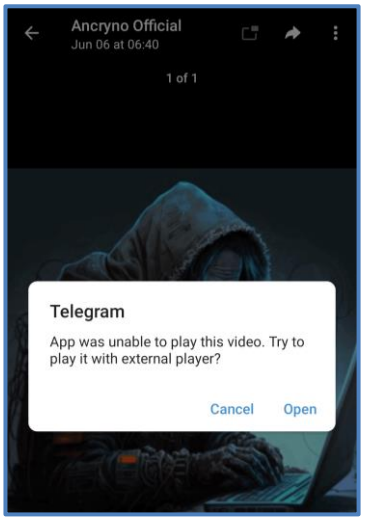
El 22 de julio de 2024, se hizo pública una grave vulnerabilidad en Telegram para Android, conocida como 'EvilVideo', que permitió a atacantes enviar APKs maliciosos disfrazados como archivos de vídeo. Esta vulnerabilidad fue inicialmente descubierta y vendida por un actor de amenazas apodado 'Ancryno' en el foro de hacking de habla rusa XSS desde el 6 de junio de 2024, señalando que el fallo existía en la versión 10.14.4 y anteriores de la aplicación.

## 2. DETALLES:

El descubrimiento de este exploit dio lugar a un análisis exhaustivo por parte de ESET, que dio como resultado un informe detallado en Telegram el 26 de junio de 2024. Sin embargo, los detalles de la vulnerabilidad recién se publicaron el 22 de julio de 2024.

ESET descubrió que el exploit EvilVideo se anunciaba en un foro clandestino, donde el vendedor proporcionó capturas de pantalla y un video que demostraba el exploit en un canal público de Telegram. Esta información le permitió a ESET rastrear el canal y obtener el payload para realizar más pruebas.

El análisis reveló que el exploit afecta a las versiones 10.14.4 y anteriores de Telegram. El payload, probablemente creado mediante la API de Telegram, se hace pasar por un archivo multimedia.




Cuando se comparte en un chat, el payload malicioso aparece como un video de 30 segundos. De forma predeterminada, Telegram descarga automáticamente los archivos multimedia, lo que significa que los usuarios con esta configuración habilitada descargarían automáticamente el payload malicioso al abrir la conversación.

Para los usuarios con la descarga automática desactivada, un solo toque en la vista previa del video iniciará la descarga del archivo.

Si un usuario intenta reproducir el “video”, Telegram muestra un mensaje de error que sugiere el uso de un reproductor externo. Al pulsar el botón Abrir en este mensaje, se solicita la instalación de una aplicación maliciosa disfrazada de reproductor externo. La aplicación en cuestión se llama "xHamster Premium Mod". Telegram luego solicita al usuario que habilite la instalación de aplicaciones desconocidas, lo que conduce a la instalación de la aplicación maliciosa.

Telegram respondió a la divulgación de ESET y lanzó una actualización el 11 de julio de 2024, que corrigió la vulnerabilidad en las versiones 10.14.5 y superiores. El parche lanzado por Telegram garantiza que los archivos compartidos se identifiquen correctamente como aplicaciones en lugar de videos.

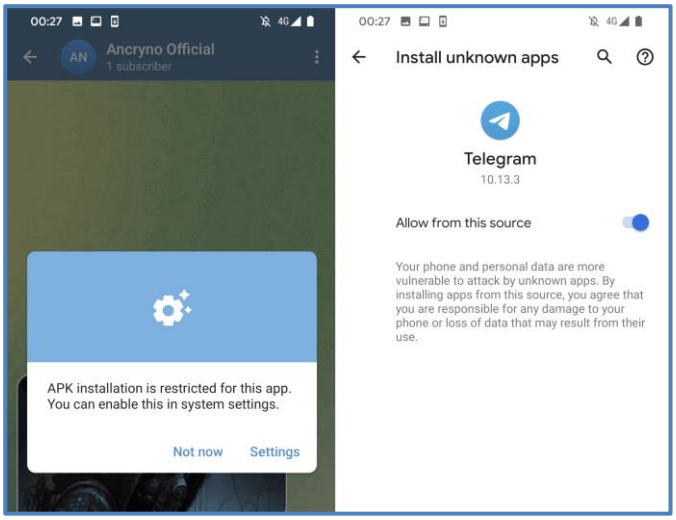
Cabe indicar que ESET probó el exploit en el cliente web de Telegram y en Telegram Desktop, y descubrió que no funcionaba allí, ya que la carga útil se trataba como un archivo de video MP4.

Si bien no está claro si la falla fue explotada activamente en los ataques, ESET compartió un servidor de comando y control (C2) utilizado por las cargas útiles en 'infinityhackscharan.ddns[.]net'.

BleepingComputer encontró dos archivos APK maliciosos usando ese C2 en VirusTotal que pretenden ser Avast Antivirus o un 'xHamster Premium Mod'.

**Indicadores de Compromiso:**

- infinityhackscharan.ddns[.]net
- xHamster Premium Mod APK
- Hash SHA-256: 843745687713d99638a27c3e3caa2777df5ec169227ec51b8e778402528f47a6
- Antivirus Avast.apk
- Hash SHA-256: 8bb90de7e397872fb721f7836982b6308d90536c63736e16b604e7830c5f3003




## 3. RECOMENDACIONES:

- Realizar el bloqueo de los indicadores de compromiso listados.
- Actualizar su aplicación a la última versión para protegerse contra EvilVideo y amenazas similares.
- Realizar un escaneo del sistema de archivos utilizando una suite de seguridad móvil para localizar y eliminar las cargas útiles de su dispositivo. Los archivos de vídeo de Telegram generalmente se almacenan en '/storage/emulated/0/Telegram/Telegram Video/' (almacenamiento interno) o en '/storage/<ID de la tarjeta SD>/Telegram/Telegram Video/' (almacenamiento externo).
- 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 como Google Play.
- Verificar los permisos que solicita una aplicación cuando se instala y asegurarse de otorgar su consentimiento solo a aquellos necesarios para la funcionalidad principal de la aplicación. Asegurarse de que Play Protect esté habilitado en todo momento, para evitar la instalación de software malicioso.
- Desactivar la descarga automática de archivos.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad y sobre los riesgos de descargar aplicaciones de fuentes no confiables.

| | |
|---|---|
| **Fuente de Información:** | • hxxps://hackread.com/telegram-android-vulnerability-evilvideo-malware-videos/<br>• hxxps://devel.group/blog/descubierto-un-zero-day-en-telegram-que-permite-enviar-apks-maliciosos-disfrazados-de-videos/<br>• hxxps://www.welivesecurity.com/es/investigaciones/evilvideo-exploit-permite-distribuir-archivos-maliciosos-videos-telegram/<br>• hxxps://www.bleepingcomputer.com/news/security/telegram-zero-day-allowed-sending-malicious-android-apks-as-videos/ |

| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°170 | Fecha: 22-07-2024 |
|---|---|---|
| | | Página: 6 de 9 |

| | | | |
|---|---|---|---|
| Componente que reporta | DIRECCIÓN NACIONAL DE INTELIGENCIA | | |
| Nombre de la alerta | Vulnerabilidad de Util-linux en productos NetApp | | |
| 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 generación de mensajes de error que contienen información confidencial que afecta a los productos NetApp. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la divulgación de información confidencial.

## 2. DETALLES:

Varios productos de NetApp incorporan Util-linux. Las versiones de Util-linux anteriores a la versión 2.37.4 son susceptibles a una vulnerabilidad que, si se explota con éxito, podría dar lugar a la divulgación de información confidencial.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2022-0563 de tipo generación de mensajes de error que contienen información confidencial en productos NetApp, se debe a una falla en las utilidades chfn y chsh de Util-linux cuando se compilan con soporte de Readline.

La biblioteca Readline usa una variable de entorno "INPUTRC" para obtener una ruta al archivo de configuración de la biblioteca. Cuando la biblioteca no puede analizar el archivo especificado, imprime un mensaje de error que contiene datos del archivo. Esta falla permite que un usuario sin privilegios lea archivos propiedad de root, lo que puede llevar a una escalada de privilegios.

### A. Productos afectados:

- Util-linux anteriores a la versión 2.37.4.
- ONTAP Select Deploy administration utility, anteriores a la versión 9.15.1.

## 3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad. Las correcciones de software se encuentran disponibles a través del sitio web de soporte de NetApp en la sección “Descarga de software”.

| | |
|---|---|
| Fuente de Información: | • hxxps://security.netapp.com/advisory/ntap-20220331-0002/<br>• hxxps://lore.kernel.org/util-linux/20220214110609.msiwlm457ngoic6w%40ws.net.home/T/#u<br>• hxxps://security.gentoo.org/glsa/202401-08<br>• hxxps://mysupport.netapp.com/site/downloads/ |

| | | |
|---|---|---|
| DINI | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°170 | Fecha: 22-07-2024<br>Página: 7 de 9 |

| | | | |
|---|---|---|---|
| Componente que reporta | DIRECCIÓN NACIONAL DE INTELIGENCIA | | |
| Nombre de la alerta | Vulnerabilidad de inyección de entidad externa XML en IBM PowerVM NovaLink | | |
| 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 Inyección de entidad externa XML (XXE) en IBM PowerVM NovaLink. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto obtener acceso a información confidencial.

## 2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-22354 de tipo inyección de entidad externa XML en IBM PowerVM NovaLink, podría permitir a un atacante remoto obtener acceso a información confidencial. La vulnerabilidad existe debido a una validación insuficiente de la entrada XML proporcionada por el usuario. Un atacante remoto puede pasar un código XML especialmente diseñado a la aplicación afectada y ver el contenido de archivos arbitrarios en el sistema o iniciar solicitudes a sistemas externos.

La explotación exitosa de la vulnerabilidad puede permitir a un atacante ver el contenido de un archivo arbitrario en el servidor o realizar un escaneo de red de la infraestructura interna y externa.

### A. Productos afectados:

- PowerVM NovaLink: anterior a 2.2.1-240626.

## 3. RECOMENDACIÓN:

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

| | |
|---|---|
| Fuente de Información: | • hxxp://www.ibm.com/support/pages/node/7159507<br>• hxxps://exchange.xforce.ibmcloud.com/vulnerabilities/280401<br>• hxxps://www.ibm.com/support/pages/node/7148426<br>• hxxps://cve.org/CVERecord?id=CVE-2024-22354 |

| | | |
|---|---|---|
| DINI | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°170 | Fecha: 22-07-2024<br>Página: 8 de 9 |

| | | | |
|---|---|---|---|
| Componente que reporta | DIRECCIÓN NACIONAL DE INTELIGENCIA | | |
| Nombre de la alerta | Actualización de Red Hat Enterprise Linux 9 para Firefox | | |
| 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:

Red Hat Product Security ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo desbordamiento de búfer y condición de carrera en la asignación de permisos en Red Hat Enterprise Linux 9 para Firefox. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto eludir las restricciones de seguridad, ejecutar código arbitrario en el sistema de destino y realizar un ataque de denegación de servicio (DoS).

## 2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-6604 de tipo desbordamiento de búfer, podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino. La vulnerabilidad existe debido a un error de límite al procesar contenido HTML. Un atacante remoto puede crear un sitio web especialmente diseñado, engañar a la víctima para que lo abra, provocar una corrupción de memoria y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-6601 de tipo condición de carrera en la asignación de permisos, podría permitir a un atacante remoto eludir las restricciones de seguridad implementadas. La vulnerabilidad existe debido a una condición de carrera en la asignación de permisos. Un atacante remoto puede engañar a la víctima para que visite un sitio web especialmente diseñado, eludir la obtención de permisos del origen de nivel superior por parte de un contenedor de origen cruzado y obtener acceso a información confidencial.

La vulnerabilidad de severidad **baja,** identificada por MITRE como CVE-2024-6603 de tipo desbordamiento de búfer, podría permitir a un atacante remoto realizar un ataque de DoS. La vulnerabilidad existe debido a un error de límite en la creación de subprocesos. Un atacante remoto puede crear un sitio web especialmente diseñado, engañar a la víctima para que lo abra, provocar una corrupción de memoria y bloquear el navegador.

### A. Productos afectados:

- Servidor Red Hat Enterprise Linux - AUS: 9.2.
- Red Hat Enterprise Linux para IBM z Systems: soporte de actualización ampliado: 9.2.
- Red Hat Enterprise Linux para Power, little endian: compatibilidad con actualizaciones extendidas: 9.2.
- Red Hat Enterprise Linux para ARM 64: compatibilidad con actualizaciones ampliada: 9.2.
- Red Hat Enterprise Linux Server para Power LE: servicios de actualización para soluciones SAP: 9.2.
- Red Hat Enterprise Linux para x86_64: compatibilidad con actualizaciones ampliada: 9.2.
- Firefox (paquete Red Hat): anterior a 115.13.0-3.el9_2.

## 3. RECOMENDACIÓN:

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

| | |
|---|---|
| Fuente de Información: | • hxxp://access.redhat.com/errata/RHSA-2024:4673<br>• hxxps://access.redhat.com/articles/11258 |

# Índice alfabético