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

186-2024-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°186	Fecha: 13-08-2024
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Hallan un nuevo malware que se sirve de extensiones falsas para Chrome y Edge		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

El equipo de investigación de la firma ReasonLabs ha dado la voz de alarma sobre la existencia de una campaña de malware generalizada que instala extensiones falsas de Google Chrome y Microsoft Edge. Lo haría mediante un troyano y a través de webs falsas que pretenden camuflarse como programas y aplicaciones populares. Dicho malware existe desde el año 2021 en sitios web de descarga con complementos para juegos y vídeos en línea.

2. DETALLES:

"El malware troyano contiene diferentes elementos que van desde simples extensiones de adware que secuestran búsquedas hasta scripts maliciosos más sofisticados que entregan extensiones locales para robar datos privados y ejecutar varios comandos", dijo el equipo de investigación de ReasonLabs en su informe sobre su análisis.

El alcance es de al menos 300.000 usuarios de Google Chrome y Microsoft Edge, lo que indica que la actividad tuvo un amplio impacto, ya que, la campaña, impulsó la instalación de software conocido como Roblox FPS Unlocker, YouTube, VLC media player, Steam o KeePass para engañar a los usuarios que buscan estos programas para que descarguen un troyano, que sirve como conducto para instalar las extensiones del navegador.

Todo comienza descargando un programa infectado desde Google. Por desgracia, los anuncios que aparecen en los resultados de búsqueda de Google resultan una vía de infección que los atacantes están utilizando cada vez más. Lo que hacen es publicar anuncios que parecen ser enlaces de descarga auténticos.

Los instaladores maliciosos firmados digitalmente registran una tarea programada que, a su vez, está configurada para ejecutar un script de PowerShell responsable de descargar y ejecutar la carga útil de la siguiente etapa obtenida de un servidor remoto.

El malware, una vez dentro del sistema, puede modificar el Registro de Windows para forzar la instalación de extensiones de la Chrome Web Store y complementos de Microsoft Edge, que son capaces de secuestrar consultas de búsqueda en Google y Microsoft Bing y redirigirlas a través de servidores controlados por atacantes.

El usuario no puede desactivar la extensión, ni siquiera con el modo de desarrollador activado. Las versiones más nuevas del script eliminan las actualizaciones del navegador.

También lanza una extensión local que se descarga directamente desde un servidor de comando y control (C2), y viene con amplias capacidades para interceptar todas las solicitudes web y enviarlas al servidor, recibir comandos y scripts cifrados, e inyectar y cargar scripts en todas las páginas.

La amenaza también es capaz de secuestrar las consultas de búsqueda de Ask.com, Bing y Google y las canaliza a través de sus servidores y después a otros motores de búsqueda.

Las consecuencias de ser víctima de este malware se listan a continuación:

- **Robo de datos:** Las extensiones maliciosas pueden robar información personal, contraseñas, datos de tarjetas de crédito e historial de navegación. Esto se usaría para el robo de identidad, fraude financiero y otros fines maliciosos.
- **Adware y ventanas emergentes:** Estas extensiones a menudo bombardean a los usuarios con anuncios y ventanas emergentes intrusivos, lo que interrumpe la experiencia de navegación y potencialmente provoca más infecciones.

- **Secuestro del navegador:** El malware puede modificar la configuración del navegador, cambiar la página de inicio, el motor de búsqueda predeterminado y la página de nueva pestaña. Esto puede resultar extremadamente frustrante y dificultar la recuperación del control del navegador.
- **Cryptojacking:** En algunos casos, el malware puede usar secretamente la potencia de procesamiento de su computadora para minar criptomonedas, lo que ralentiza su dispositivo y aumenta sus facturas de electricidad.

3. RECOMENDACIONES:

- Analizar el sistema con un antivirus actualizado.
- Cambiar y utilizar contraseñas fuertes y únicas para cada cuenta.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Eliminar la tarea programada que reactiva el malware cada día, eliminar las claves del Registro y suprimir estos archivos y carpetas del sistema:
  - C:\Windows\system32\Bloqueador de privacidadwindows.ps1
  - C:\Windows\system32\Windowsupdater1.ps1
  - C:\Windows\system32\WindowsUpdater1Script.ps1
  - C:\Windows\system32\Optimizerwindows.ps1
  - C:\Windows\system32\Printworkflowservice.ps1
  - C:\Windows\system32\NvWinSearchOptimizer.ps1 - versión 2024
  - C:\Windows\system32\kondserp_optimizer.ps1 - Versión de mayo de 2024
  - C:\Windows\Grid interno del kernel
  - C:\Windows\InternalKernelGrid3
  - C:\Windows\InternalKernelGrid4
  - C:\Windows\ShellServiceLog
  - C:\windows\protectorlog de privacidad
  - C:\Windows\NvOptimizerLog
- Descargar software únicamente de sitios web confiables y de buena reputación. Evitar hacer clic en enlaces o anuncios sospechosos, que provengan de correos electrónicos, mensajes de texto o mensajes de redes sociales que soliciten información personal.
- Tener cuidado con las extensiones del navegador. Revisar los permisos solicitados por cualquier extensión antes de instalarla. Desconfiar de las extensiones que solicitan un acceso excesivo a sus datos.
- Mantener el software actualizado. Actualizar periódicamente el sistema operativo, navegador y software antivirus para protegerse contra las últimas amenazas.
- Utilizar una solución antivirus confiable que pueda ayudar a detectar y bloquear software malicioso.
- Considerar utilizar un administrador de contraseñas dedicado para proteger su información confidencial.
- Realizar copias de seguridad de sus datos importantes periódicamente para minimizar el impacto de un posible ataque.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://www.escudodigital.com/ciberseguridad/hallan-nuevo-malware-extensiones-falsas-chrome-edge_60066_102.html • hxxps://www.linkedin.com/pulse/cuidado-nuevo-malware-ataca-300000-usuarios-con-extensiones-falsas-yspzc/ • hxxps://ciberprisma.org/2024/08/11/una-nueva-campana-de-malware-ataco-a-300-000-usuarios-con-extensiones-falsas-para-chrome-y-edge/ • hxxps://www.adslzone.net/noticias/seguridad/nuevo-virus-chrome-edge-extensiones-infectadas-0824/ • hxxps://www.hardreset.info/es/articles/malware-masquerade-rogue-chrome-and-edge-extensions-infect-300000-users/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°186	Fecha: 13-08-2024 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en múltiples productos de Rockwell Automation		
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 validación de entrada incorrecta en múltiples productos de Rockwell Automation. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto bloquear el dispositivo al que se accede.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-7515 de tipo validación de entrada incorrecta en múltiples productos de Rockwell Automation, podría permitir a un atacante remoto bloquear el dispositivo al que se accede. Existe una vulnerabilidad de denegación de servicio en los productos afectados. Un paquete de administración PTP mal formado puede provocar una falla grave e irrecuperable en el controlador.

A. Productos afectados:

- CompactLogix 5380 (5069 - L3z): versiones anteriores a v36.011, v35.013, v34.014.
- CompactLogix 5480 (5069 - L4): versiones anteriores a v36.011, v35.013, v34.014.
- ControlLogix 5580 (1756 - L8z): versiones anteriores a v36.011, v35.013, v34.014.
- GuardLogix 5580 (1756 - L8z): versiones anteriores a v36.011, v35.013, v34.014.
- Compact GuardLogix 5380 (5069 - L3zS2): versiones anteriores a v36.011, v35.013, v34.014.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad. Actualizar los productos a v36.011, v35.013, v34.014 o posterior.
- Restringir la comunicación al objeto CIP 103 (0x67).
- Implementar las mejores prácticas de seguridad sugeridas por Rockwell Automation para minimizar el riesgo de vulnerabilidad.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-226-10 • hxxps://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1085012/loc/en_US#__highlight

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°186	Fecha: 13-08-2024 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en SuiteLink Server de AVEVA		
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 asignación de recursos sin límites ni limitaciones que afecta al SuiteLink Server de AVEVA. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto hacer que el servidor consuma recursos excesivos del sistema, impidiendo el procesamiento de mensajes de SuiteLink en el host objetivo.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-7113 de tipo asignación de recursos sin límites ni limitaciones que afecta al servidor SuiteLink de AVEVA, podría provocar que un servidor SuiteLink consuma recursos excesivos del sistema y ralentice el procesamiento de E/S de datos mientras dure el ataque.

A. Productos afectados:

- SuiteLink: versión 3.7.0 y anteriores.
- Historian: versión 2023 R2 P01 y anteriores.
- InTouch: versión 2023 R2 P01 y anteriores.
- Application Server: versión 2023 R2 P01 y anteriores.
- Communication Drivers Pack: versión 2023 R2 y anteriores.
- Batch Management: versión 2023 y anteriores.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad. Las organizaciones evalúen el impacto de estas vulnerabilidades en función de su entorno operativo, arquitectura e implementación de productos.
- Aplicar las actualizaciones de seguridad lo antes posible, para los usuarios con las versiones de productos afectadas.
- Aplicar reglas de firewall de host o red que restrinjan al servidor SuiteLink a aceptar tráfico solo de fuentes confiables. De manera predeterminada, SuiteLink escucha en el puerto 5413.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-226-01 • hxxp://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-7113

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°186	Fecha: 13-08-2024
		Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en Adobe Photoshop		
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 uso posterior a la liberación en Adobe Photoshop. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto comprometer el sistema vulnerable.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-34117 de tipo uso posterior a la liberación en Adobe Photoshop, podría permitir a un atacante remoto comprometer el sistema vulnerable. La vulnerabilidad existe debido a un error de uso después de la liberación al manipular archivos. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado, desencadenar un error de uso después de la liberación y ejecutar código arbitrario en el sistema.

La explotación exitosa de la vulnerabilidad podría permitir a un atacante comprometer el sistema vulnerable.

A. Productos afectados:

- Adobe Photoshop: 20.0 - 25.9.1.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxp://helpx.adobe.com/security/products/photoshop/apsb24-49.html

Índice alfabético