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

209-2024-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°209	Fecha: 10-09-2024
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Nuevo ataque RAMBO utiliza señales de radio RAM para robar datos de redes aisladas		
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		

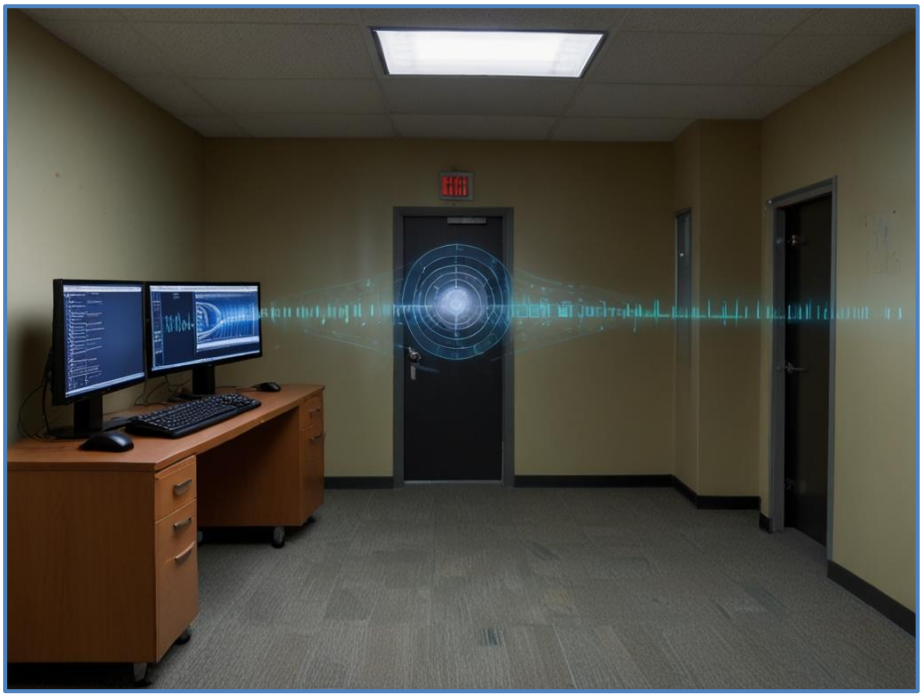
Descripción

1. ANTECEDENTES:

En el campo de la ciberseguridad, los sistemas "air-gapped" han sido considerados durante mucho tiempo una de las defensas más efectivas para proteger información crítica. Estos sistemas están físicamente aislados de redes externas, haciéndolos virtualmente inaccesibles a ataques remotos.

Sin embargo, un nuevo método de exfiltración de datos ha demostrado que, incluso en entornos air-gapped, la información no está completamente a salvo.

Se ha descubierto un nuevo ataque de canal lateral que aprovecha las señales de radio emanadas de la memoria de acceso aleatorio (RAM) de un dispositivo como mecanismo de exfiltración de datos, lo que representa una amenaza para las redes con espacios de aire.



2. DETALLES:

Este método, conocido como RAMBO (Random Access Memory Based Oscillations), aprovecha las emisiones de radiofrecuencia generadas por la actividad en la memoria RAM del sistema. Este ataque demuestra que el funcionamiento regular de los chips de memoria DRAM produce pequeñas emisiones de radiofrecuencia que pueden ser captadas y traducidas en datos legibles.

Para llevar a cabo el ataque RAMBO, un atacante coloca malware en la computadora aislada para recopilar datos confidenciales y prepararlos para la transmisión. El malware puede codificar diferentes tipos de información, como archivos, imágenes, registros de pulsaciones de teclas, información biométrica y claves de cifrado.

Transmite los datos manipulando patrones de acceso a la memoria (operaciones de lectura/escritura en el bus de memoria) para generar emisiones electromagnéticas controladas desde la RAM del dispositivo.

Estas emisiones son esencialmente un subproducto del malware que cambia rápidamente las señales eléctricas dentro de la RAM, un proceso que los productos de seguridad no monitorean activamente y no se puede marcar ni detener.

Los datos emitidos se codifican en "1" y "0", representados en las señales de radio como "encendido" y "apagado".

Un receptor a cierta distancia, con un hardware de radio definido por software (SDR) y una antena comercial sencilla, puede capturar estas emisiones y reconstruir los datos que se encuentran en la memoria del sistema, incluso si está físicamente aislado.

Los investigadores optaron por utilizar el código Manchester para mejorar la detección de errores y garantizar la sincronización de la señal, reduciendo las posibilidades de interpretaciones incorrectas por parte del receptor.

El atacante puede utilizar una radio definida por software (SDR) relativamente económica con una antena para interceptar las emisiones electromagnéticas moduladas y convertirlas nuevamente en información binaria.

Como siempre ocurre con los ataques de este tipo, es necesario que la red aislada se vea primero comprometida a través de otros medios (como un infiltrado malintencionado, unidades USB envenenadas o un ataque a la cadena de suministro), lo que permite que el malware active el canal encubierto de exfiltración de datos.

A lo largo de los años, el Dr. Mordechai Guri, jefe del Laboratorio de Investigación Cibernética Ofensiva del Departamento de Ingeniería de Software y Sistemas de Información de la Universidad Ben-Gurion del Negev en Israel, ha inventado varios mecanismos para extraer datos confidenciales de redes fuera de línea aprovechando cables Serial ATA (SATAn), giroscopio MEMS (GAIROSCOPE), LED en tarjetas de interfaz de red (ETHERLED) y consumo de energía dinámico (COVID-bit).

Algunos de los otros enfoques no convencionales ideados por el investigador implican la filtración de datos de redes aisladas a través de señales acústicas encubiertas generadas por ventiladores de la unidad de procesamiento de gráficos (VENTILADOR DE GPU), ondas ultrasónicas producidas por los zumbadores integrados en la placa base (EL GRILLO), e incluso paneles de visualización de la impresora y luces de estado (Fuga de impresora).

3. RECOMENDACIONES:

- Aplicar restricciones de zona "rojo-negro" para la transferencia de información.
- Usar un sistema de detección de intrusos (IDS).
- Implementar la monitorización del acceso a la memoria a nivel de hipervisor.
- Utilizar bloqueadores de radio para bloquear las comunicaciones inalámbricas.
- Configurar restricciones de zona estrictas para mejorar la defensa física, interferencia de RAM para interrumpir los canales encubiertos en la fuente, interferencia de EM externa para interrumpir las señales de radio y recintos de Faraday para impedir que los sistemas con espacios de aire emanen radiación EM externamente.

Fuente de Información:	• hxxps://thehackernews.com/2024/09/new-rambo-attack-uses-ram-radio-signals.html • hxxps://unaaldia.hispasec.com/2024/09/nuevas-tecnicas-de-exfiltracion-de-datos-en-sistemas-aislados-pixhell-y-rambo.html • hxxps://blog.segu-info.com.ar/2024/09/ataque-rambo-roba-datos-usando-ram-en.html?m=0 • hxxps://randomaccessnoticias.com/el-nuevo-ataque-rambo-utiliza-senales-de-radio-ram-para-robar-datos-de-redes-aisladas/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°209	Fecha: 10-09-2024
		Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el Servidor web SCADA SpiderControl de iniNet Solutions GmbH		
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 Instituto de Investigación Elex Feigong de Elex CyberSecurity, Inc. ha reportado una vulnerabilidad de severidad **ALTA** de tipo carga sin restricciones de archivos de tipo peligroso que afecta al Servidor web SCADA SpiderControl de iniNet Solutions GmbH, un programa HMI. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto iniciar sesión o ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

El servidor web SCADA SpiderControl es una herramienta versátil y potente diseñada para integrar y gestionar sistemas de automatización industrial. Funciona a través de un navegador HTML5 estándar, lo que permite a los usuarios desarrollar y gestionar interfaces hombre-máquina (HMI) y sistemas de control de supervisión y adquisición de datos (SCADA) de forma eficaz.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-8232 de tipo carga sin restricciones de archivos en el servidor web SpiderControl SCADA, podría permitir a un atacante cargar archivos maliciosos especialmente diseñados sin autenticación.

A. Productos afectados:

- Servidor web SCADA SpiderControl: versiones v2.09 y anteriores.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la nueva versión de SpiderControl SCADA Server (3.2.2) que el proveedor IniNet Solutions ha lanzado para abordar esta vulnerabilidad.
- No conectar el software del sistema de control directamente a Internet, ya que el servidor web está diseñado para ser utilizado en un entorno protegido. Si un usuario debe conectarse a Internet, IniNet Solutions GmbH recomienda utilizar una infraestructura administrada para ello.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-254-02 • hxxps://spidercontrol.net/download/download-area-2/?lang=en

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°209	Fecha: 10-09-2024 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el software SequenceManager 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:

La empresa Rockwell Automation, Inc. ha reportado una vulnerabilidad de severidad **ALTA** de tipo ruta de búsqueda o elemento sin comillas que afecta a su software de procesamiento por lotes y secuenciación basada en controlador Logix "SequenceManager". La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado generar una condición de denegación de servicio (DoS).

2. DETALLES:

SequenceManager es una solución de software que ofrece funciones de control y secuenciación por lotes para controladores basados en Logix. Permite a los usuarios configurar operaciones en Studio 5000 Logix Designer, ejecutar secuencias en FactoryTalk View SE y capturar y visualizar resultados por lotes.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2024-4609 de tipo ruta de búsqueda o elemento sin comillas, podría permitir que un usuario malintencionado envíe paquetes malformados al servidor y provoque una condición de DoS. Si se explota, el dispositivo dejaría de responder y sería necesario reiniciarlo manualmente para recuperarlo. Además, si se explota, podría perderse la vista de las secuencias de equipos posteriores en el controlador. Los usuarios no podrían ver el estado ni ordenar las secuencias de equipos, pero la secuencia de equipos seguiría ejecutándose sin interrupciones.

A. Productos afectados:

- SequenceManager: versiones anteriores a la 2.0.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 2.0 o superior que aborda esta vulnerabilidad. No existe ninguna una solución disponible para estas vulnerabilidades en las versiones de software afectadas anteriores a la v2.0.
- Aplicar las mejores prácticas de seguridad, siempre que sea posible, para los casos donde las versiones del software no hayan podido ser actualizadas.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-254-03 • hxxps://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1085012/loc/en_US#__highlight

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°209	Fecha: 10-09-2024
		Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en Microsoft Servicing Stack		
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 uso después de la liberación en Microsoft Servicing Stack. La explotación exitosa de esta vulnerabilidad podría exponer los sistemas afectados a varios ataques. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante la ejecución remota de código sin necesidad de interacción del usuario, lo que puede provocar un compromiso total del sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-43491 de tipo uso después de la liberación en Microsoft Servicing Stack, ha revertido las correcciones para vulnerabilidades mitigadas previamente en sistemas Windows 10, versión 1507 (Windows 10 Enterprise 2015 LTSB y Windows 10 IoT Enterprise 2015 LTSB) que han instalado la actualización de seguridad de Windows publicada el 12 de marzo de 2024 (KB5035858, compilación del SO 10240.20526) u otras actualizaciones publicadas hasta agosto de 2024.

Esta vulnerabilidad reintroduce vulnerabilidades mitigadas anteriormente, lo que podría exponer los sistemas afectados a varios ataques. La explotación exitosa de esta vulnerabilidad podría permitir la ejecución remota de código sin necesidad de interacción del usuario, lo que puede provocar un compromiso total del sistema. La vulnerabilidad se está explotando activamente en la naturaleza por múltiples actores de amenazas.

Nota: Windows 10, versión 1507, alcanzó el fin del soporte (EOS) el 9 de mayo de 2017 para dispositivos con las ediciones Pro, Home, Enterprise, Education y Enterprise IoT. Solo las ediciones Windows 10 Enterprise 2015 LTSB y Windows 10 IoT Enterprise 2015 LTSB siguen recibiendo soporte.

A. Productos afectados:

- Sólo a Windows 10 versión 1507; todas las versiones posteriores de Windows 10 no se ven afectadas.

3. RECOMENDACIÓN:

- Actualizar el producto afectado con los últimos parches de seguridad de software disponible que aborda esta vulnerabilidad.
- Instalar las dos actualizaciones en un orden específico: primero instalar la actualización de la pila de servicio de septiembre de 2024 (SSU KB5043936) y luego la actualización de seguridad de Windows de septiembre de 2024 (KB5043083). Es fundamental instalarlas en el orden especificado.
- Considerar aislar los sistemas afectados de la red para minimizar el riesgo de explotación, en los casos en que no haya sido posible aplicar los parches de inmediato.
- Supervisar los sistemas para detectar cualquier actividad sospechosa que pueda indicar la explotación de las vulnerabilidades reintroducidas.
- Considerar actualizar de Windows 10 versión 1507 a una versión más reciente y compatible de Windows, ya que esta versión ha llegado al final del soporte para la mayoría de las ediciones.
- Planificar la migración a versiones actuales y compatibles lo antes posible, para las organizaciones que aún usan Windows 10 Enterprise 2015 LTSB o Windows 10 IoT Enterprise 2015 LTSB.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-43491 • hxxps://vuldb.com/?id.277088&utm_source=feedly • hxxps://vulnera.com/newswire/microsofts-september-2024-patch-tuesday-addresses-79-security-flaws-including-4-zero-days/

Índice alfabético