PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 27 de marzo de 2024

075-2024-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 Aérea del 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 las empresas 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°075	Fecha: 27-03-2024
		Página: 4 de 9

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	INC Ransomware ataca al Servicio Nacional de Salud de Escocia y amenaza con filtrar 3 TB de datos de pacientes		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

La banda INC Ransomware, que surgió en julio de 2023, es un actor de amenazas relativamente nuevo que emplea varias tácticas. Son conocidos por cifrar los datos de una víctima y exigir un pago de rescate por descifrarlos. de lo contrario, amenazan con filtrar públicamente la información robada si no se paga el rescate. Informes recientes indican un enfoque en las instituciones de salud, intensificando la urgencia de pagar debido a la naturaleza sensible de los datos robados, como los registros de los pacientes.

A pesar de que surgieron en julio de 2023, los ataques INC no han sido ampliamente reportados, lo que indica una actividad limitada. Sin embargo, mantienen presencia en la web oscura, donde filtran datos de víctimas robadas y posiblemente comunican demandas de rescate.

2. DETALLES:

La banda mencionada supuestamente se ha dirigido al Servicio Nacional de Salud de Escocia, comúnmente conocido como NHS Scotland. En un anuncio reciente en su blog de filtraciones en la web oscura, el grupo de ransomware afirmó haber robado con éxito la cantidad de 3 terabytes de datos confidenciales. Han amenazado con publicar estos datos si no se cumplen sus demandas.

Los operadores del ransomware INC proporcionaron un "paquete de prueba" que consta de 14 capturas de pantalla. Estas capturas de pantalla parecen mostrar los registros de los pacientes, como cartas e intercambios de correo electrónico sobre su salud, que involucran a médicos generales (GP) de varias clínicas y hospitales de todo el país.

Estos indicios han puesto al grupo en el centro de atención dentro de la comunidad de ciberseguridad, las instituciones sanitarias y los principales medios de comunicación.

Al momento de escribir este artículo, NHS Scotland no ha confirmado la ocurrencia del ataque de ransomware ni si ha experimentado una violación de datos. Sin embargo, si la institución reconoce el ciberataque, los pacientes deben prepararse para recibir noticias potencialmente preocupantes sobre la seguridad de su información.

3. RECOMENDACIONES:

- Ejecutar la estrategia 3-2-1 de copias de seguridad, que consiste en realizar tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Mantener siempre actualizado los programas, tanto en los dispositivos como en los servidores, para evitar que los atacantes aprovechen las vulnerabilidades y se infiltren en su red.
- Utilizar un software antivirus confiable y mantenerlo activo y actualizado.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.

Fuente de Información:	• hxxps://www.hackread.com/inc-ransomware-nhs-scotland-3tb-patient-data-leak/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°075**	**Fecha: 27-03-2024**
		Página: 5 de 9

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Arena Simulation 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:

Michael Heinzl ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo escritura fuera de límites, desbordamiento de búfer basado en montón, restricción inadecuada de operaciones dentro de los límites de un búfer de memoria, usar después de free, acceso al puntero no inicializado y lectura fuera de límites en Arena Simulation de Rockwell Automation. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-21912 de tipo escritura fuera de límites, podría permitir que un usuario malintencionado inserte código no autorizado en el software. Esto se hace escribiendo más allá del área de memoria designada, lo que provoca una infracción de acceso. Una vez dentro, el actor de la amenaza puede ejecutar código dañino en el sistema. Esto afecta la confidencialidad, integridad y disponibilidad del producto. Para desencadenar esto, el usuario tendría que abrir, sin saberlo, un archivo malicioso compartido por el actor de la amenaza.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-21913 de tipo desbordamiento de búfer basado en montón, podría permitir que un usuario malintencionado inserte código no autorizado en el software al sobrepasar los límites de la memoria, lo que desencadena una infracción de acceso. Una vez dentro, el actor de la amenaza puede ejecutar código dañino en el sistema. Esto afecta la confidencialidad, integridad y disponibilidad del producto. Para desencadenar esto, el usuario tendría que abrir, sin saberlo, un archivo malicioso compartido por el actor de la amenaza.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-2929 de tipo restricción inadecuada de operaciones dentro de los límites de un búfer de memoria, podría permitir potencialmente que un usuario malintencionado inserte código no autorizado en el software corrompiendo la memoria y provocando una infracción de acceso. Una vez dentro, el actor de la amenaza puede ejecutar código dañino en el sistema. Esto afecta la confidencialidad, integridad y disponibilidad del producto. Para desencadenar esto, el usuario tendría que abrir, sin saberlo, un archivo malicioso compartido por el actor de la amenaza.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-21918 de tipo usar después de free, podría permitir potencialmente que un usuario malintencionado inserte código no autorizado en el software corrompiendo la memoria y provocando una infracción de acceso. Una vez dentro, el actor de la amenaza puede ejecutar código dañino en el sistema. Esto afecta la confidencialidad, integridad y disponibilidad del producto. Para desencadenar esto, el usuario tendría que abrir, sin saberlo, un archivo malicioso compartido por el actor de la amenaza.

A. Productos afectados:

- Arena Simulation Software, versión 16.00.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 16.20.03 disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://www.rockwellautomation.com/en-us/support/advisory.SD-1665.html • hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-086-03

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°075	Fecha: 27-03-2024
		Página: 6 de 9

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en C-MORE EA9 HMI de Automation-Direct		
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:

Tomer Goldschmidt, de Claroty Research - Team82 ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo limitación inadecuada de un nombre de ruta a un directorio restringido (Path Traversal), desbordamiento de búfer basado en pila y almacenamiento en texto plano de una contraseña en C-MORE EA9 HMI de Automation-Direct. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante explotar un dispositivo remoto e inyectar código malicioso en el panel.

2. DETALLES:

El C-MORE EA9 HMI de AutomationDirect es una interfaz hombre-máquina (HMI) que ofrece una amplia gama de características y funcionalidades, es una opción sólida para aquellos que buscan una interfaz de usuario eficiente y fácil de usar en los sistemas de automatización industrial.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-25138 de tipo limitación inadecuada de un nombre de ruta a un directorio restringido, podría permitir a un atacante enviar una ruta relativa en la URL sin una desinfección adecuada del contenido.

Se han asignado los siguientes identificadores para las vulnerabilidades de severidad media: CVE-2024-25137, CVE-2024-25138.

A. Productos afectados:

- C-MORE EA9 HMI, versión 6.77 y anteriores de los siguientes modelos: T6CL, T7CL, T7CL-R, T8CL, T10CL, T10WCL, T12CL, T15CL, T15CL-R, RHMI y PGMSW.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión v6.78 disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-086-01

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°075**	**Fecha: 27-03-2024**
		Página: 7 de 9

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en IBM Cognos Command Center		
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 **CRÍTICA** y **MEDIA** de tipo deserialización de datos que no son de confianza, divulgación de información, secuencias de comandos entre sitios y validación de entrada incorrecta en IBM Cognos Command Center. La explotación exitosa de estas vulnerabilidades permite a un atacante remoto ejecutar código arbitrario en el sistema de destino, obtener acceso a información potencialmente confidencial, realizar ataques de secuencias de comandos entre sitios (XSS).

2. DETALLES:

IBM Cognos Command Center es una herramienta de software de IBM diseñada para administrar, monitorear y automatizar procesos dentro de un entorno de IBM Cognos. Esta plataforma permite a los usuarios supervisar el rendimiento de sus sistemas Cognos, realizar tareas administrativas y programar actividades como la generación de informes y la distribución de datos.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2023-46604 de tipo limitación inadecuada de un nombre de ruta a un directorio restringido, podría permitir a un atacante enviar una ruta relativa en la URL sin una desinfección adecuada del contenido.

Se han asignado los siguientes identificadores para las vulnerabilidades de severidad media: CVE-2023-50324, CVE-2010-2084 y CVE-2023-22081.

A. Productos afectados:

- IBM Cognos Command Center: 10.2.4.1 - 10.2.5.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://www.ibm.com/support/pages/node/7112504

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°075**	**Fecha: 27-03-2024** **Página: 8 de 9**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de DoS en múltiples productos de Cisco		
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:**

Cisco ha reportado una vulnerabilidad de severidad **ALTA** de tipo limpieza incompleta en la función de puerta de enlace DNS de multidifusión (mDNS) del software Cisco IOS XE para controladores de LAN inalámbrica (WLC). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto generar una condición de denegación de servicio (DoS).

2. **DETALLES:**

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-20303 en la función de puerta de enlace mDNS del software Cisco IOS XE para controladores de LAN inalámbrica, podría permitir que un atacante adyacente no autenticado provoque una condición de DoS.

Esta vulnerabilidad se debe a una gestión inadecuada de las entradas del cliente mDNS. Un atacante podría aprovechar esta vulnerabilidad conectándose a la red inalámbrica y enviando un flujo continuo de paquetes mDNS específicos. Un exploit exitoso podría permitir que el atacante haga que el controlador inalámbrico tenga una alta utilización de la CPU, lo que podría llevar a que los puntos de acceso (AP) pierdan su conexión con el controlador y resulte en una condición DoS.

A. Productos afectados:

Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco IOS XE, tienen habilitada la función de puerta de enlace mDNS y administran AP en modo FlexConnect:

- Controladores inalámbricos Catalyst 9800-CL para la nube.
- Controlador inalámbrico integrado Catalyst 9800 para conmutadores Catalyst series 9300, 9400 y 9500.
- Controladores inalámbricos Catalyst serie 9800.
- Controlador inalámbrico integrado en los AP Catalyst.

3. **RECOMENDACIÓN:**

- Actualizar los paquetes afectados a las últimas versiones disponibles que Cisco ha lanzado para abordar esta vulnerabilidad. Actualmente aún no hay ninguna solución oficial.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-mdns-dos-4hv6pBGf

Índice alfabético