Boletín de Ciberseguridad

Riesgo de Ransomware y Vulnerabilidades

22-Jul-2022

Sobre Axus

Axus es una empresa líder en ciberseguridad, con presencia en el Perú y Latinoamérica. Asesora a clientes en la protección de su información e infraestructura tanto en ámbitos industriales (OT) como en ámbitos corporativos (IT) y viene registrando una creciente participación en el ámbito de Internet de las Cosas (IoT) y en la protección de entornos Cloud e Híbridos.

En base a su reputación como especialista con los principales fabricantes de la industria y su equipo profesional en permanente capacitación, Axus genera valor a través de una visión consultiva que busca definir soluciones a la medida de las necesidades de cada cliente.

Resumen Ejecutivo

Ante un panorama de constantes cambios, es importante mantenernos alertas a las distintas amenazas que surgen repentinamente. Los ataques cibernéticos y grupos que los organizan aumentan cada año, por lo que es necesario mantenernos alerta a los principales programas maliciosos que se detectan y de esta manera estar preparados.

El presente boletín contiene información acerca de algunos de los principales malware detectados en las últimas semanas, como el ZuoRAT y RedAlert, así como de vulnerabilidades que están siendo explotadas por diferentes grupos de amenaza. Por el lado de la seguridad industrial, les presentamos el caso del ransomware Pipedream, dirigido principalmente a sistemas Schneider Modicon y Omron, así como vulnerabilidades críticas en sistemas del fabricante Fisto.

A continuación, compartimos con ustedes algunas de las alertas más relevantes a considerar:

Nuevo RedAlert ransomware apunta a servidores Windows, Linux VMware ESXi

Tipo de Ataque: Ransomware

Medio de Propagación: Correo electrónico, redes sociales, entre otros

1. PRODUCTOS AFECTADOS:

- Servidores Windows
- Servidores Linux VMWare ESXi

2. RESUMEN:

El equipo de Bleeping Computer, reconocido noticiero de seguridad de la información, identificó un nuevo ransomware conocido como **RedAlert**, que se dirige a los servidores Windows y Linux para robar información y chantajear a sus víctimas.

3. DETALLE:

El ransomware se denominó "RedAlert" según una cadena utilizada en la nota de rescate. El cifrado de Linux está diseñado para apuntar a los servidores VMware ESXi, con opciones de línea de comandos que permiten a los atacantes apagar todas las máquinas virtuales en ejecución antes de cifrar los archivos.

Figura 2: Opciones de comando del Ransomware RedAlert

Al ejecutar el Ransomware con el argumento '-w', el codificador de Linux apagará todas las máquinas virtuales VMware ESXi en ejecución con el siguiente comando esxcli:

esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process list | tail -n +2 | awk -F $',' '{system("esxcli vm process kill --type=force --world-id=" $1)}'

Al cifrar archivos, el ransomware utiliza el algoritmo de cifrado de clave pública **NTRUEncrypt**, que admite varios "Conjuntos de parámetros" que ofrecen diferentes niveles de seguridad.

Una característica interesante de RedAlert/N13V es la opción de línea de comandos '-x' que realiza 'pruebas de rendimiento de criptografía asimétrica' utilizando estos diferentes conjuntos de parámetros NTRUEncrypt. Sin

embargo, no está claro si hay una forma de forzar un conjunto de parámetros en particular al cifrar y/o si el ransomware seleccionará uno más eficiente.

El ransomware cifrará estos tipos de archivos y agregará la extensión .crypt658 a los nombres de archivo de los archivos cifrados. Dentro de cada carpeta, el ransomware también creará una nota de rescate personalizada llamada HOW_TO_RESTORE, que contiene una descripción de los datos robados y un enlace al sitio web de pago de rescate TOR exclusivo de la víctima. El sitio de pago Tor es similar a otros sitios de operación de ransomware, ya que muestra la demanda de rescate y proporciona una forma de negociar con los actores de amenazas.

Sin embargo, **RedAlert/N13V** solo acepta la criptomoneda Monero para el pago, que no se vende comúnmente en los intercambios de criptomonedas de EE. UU., ya que es una moneda de seguridad. Si bien solo se encontró un codificador de Linux, el sitio de pago tiene elementos ocultos que sugieren que también existen decodificadores de Windows.

Como la mayoría de las nuevas operaciones de ransomware dirigidas a empresas, RedAlert ejecuta ataques de extorsión dual, es decir, cuando se roban datos y luego se implementa ransomware para cifrar dispositivos. Esta táctica proporciona dos métodos de extorsión, lo que permite a los actores de amenazas no solo exigir un rescate para recibir un descifrador, sino también exigir uno para evitar la filtración de datos robados.

Cuando una víctima no paga una demanda de rescate, la pandilla RedAlert publica datos robados en su sitio de fuga de datos que cualquiera puede descargar. Actualmente, el sitio de fuga de datos de **RedAlert** solo contiene los datos de una organización, lo que indica que la operación es muy nueva.

Si bien no ha habido mucha actividad con la nueva operación de ransomware **N13V/RedAlert**, definitivamente tendremos que estar atentos debido a su funcionalidad avanzada y soporte inmediato tanto para Linux como para Windows.

4. RECOMENDACIONES:

- Mantener actualizado el sistema operativo e instale aplicaciones de antivirus.
- Realizar periódicamente respaldos de seguridad.
- Sensibilizar al recurso humano de su organización para que evite descargar aplicaciones sospechosas.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/new-redalert-ransomware-targets-windows-linux-vmware-esxi-servers/

Servidores de Microsoft Exchange sufren ataques de puerta trasera de SessionManager

Tipo de Ataque: Malware
Medio de Propagación: USB, Disco, Red, Correo, Navegación de Internet

1. PRODUCTOS AFECTADOS:

- Microsoft Exchange Server, todas las versiones

2. RESUMEN:

Las vulnerabilidades relacionadas al ProxyLogon en los servidores de Microsoft Exchange se han vuelto un objetivo común entre los atacantes, ya que les permite establecer puertas traseras (backdoors)a través de la configuración de módulos IIS. Particularmente, el módulo SessionManager, les permite a los atacantes mantener un backdoor resistente a actualizaciones y relativamente sigiloso para acceder a la infraestructura de TI.

3. DETALLE:

Según Kaspersky Lab, los primeros ataques de SessionManager se registraron a fines de marzo de 2021. Las víctimas de los atacantes fueron principalmente agencias gubernamentales y organizaciones sin fines de lucro en África, Asia del Sur, Europa y Medio Oriente, así como en Rusia.

Este ataque inicia con la inyección de malware de forma remota, como un módulo para Microsoft IIS (un conjunto de servicios web que incluye el servidor de correo de Exchange). Los atacantes explotan la conocida vulnerabilidad ProxyLogon para propagar SessionManager y otros módulos maliciosos de IIS.

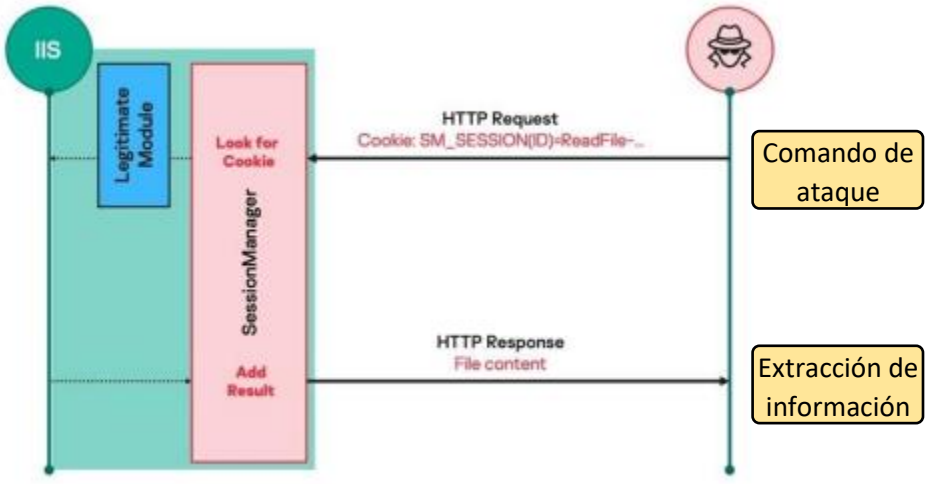

Figura 1: Módulo ISS malicioso procesando solicitudes

SessionManager proporciona "una forma ideal de implementar puertas traseras potentes, persistentes y sigilosas". Esto significa que pueden responder a solicitudes HTTP específicamente diseñadas enviadas por el operador; y a su vez, le facilita a los atacantes obtener información importante de los correos

electrónicos y acelerar su acceso. Es bastante complejo diferenciar las solicitudes HTTP normales de las maliciosas.

Una vez en la red, el malware toma el control de su dispositivo, donde el usuario ahora puede acceder a las contraseñas almacenadas en su memoria. Incluso puede instalar herramientas adicionales como el cargador de reflexivo basado en PowerSploit, Mimikat SSP, ProcDump y el motor legal de volcado de memoria Avast.

Hasta el momento, la puerta trasera se ha encontrado en 34 servidores en 24 empresas. Pero el informe señala que el SessionManager a menudo pasa desapercibido, ya que los rastreadores en línea más populares lo detectan mal.

Los analistas dicen que estos ataques probablemente estén relacionados con el grupo **Gelsemium**, citando similitudes en las muestras de malware, así como objetivos similares.

4. RECOMENDACIONES:

- Utilizar un antivirus robusto para analizar todas las descargas y archivos sospechosos. Este se debe mantener siempre actualizado y activo.
- Mantener el sistema operativo, navegador y aplicaciones siempre actualizados a su última versión para evitar vulnerabilidades.
- Utilizar contraseñas robustas y diferentes para proteger todas las cuentas. De ser posible, utilizar la autenticación multifactor.
- Tener cuidado por donde se navega, utilizar sólo webs seguras con https y certificado digital, y utilizar el modo incógnito cuando no se quiera dejar rastro.
- Controlar la descarga de aplicaciones y software para asegurar que sea legítimo. Además, controlar los permisos que tienen los usuarios sobre las aplicaciones basado en el concepto de Zero Trust.

5. REFERENCIAS:

- https://securelist.com/the-sessionmanager-iis-backdoor/106868/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26855
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27065

Nueva campaña de malware “ZuoRAT” dirigido a equipos Windows, macOS y Linux

Tipo de Ataque: Troyanos
Medio de Propagación: USB, Disco, Red, Correo, Navegación de Internet

1. PRODUCTOS AFECTADOS:

- Cisco RV320, Cisco RV325, Cisco RV420
- Asus RT-AC68U, Asus RT-AC530, Asus RT-AC68P, Asus RT-AC1900U
- DrayTek Vigor 3900 y dispositivos Netgear no especificados

2. RESUMEN:

Investigadores de Black Lotus Labs de Lumen Technologies han descubierto una nueva campaña de malware que utiliza enrutadores pequeños y medianos, también conocidos como SOHO (Small Office, Home Office), infectados para atacar principalmente redes de interés en América del Norte y Europa. Este malware es un Troyano de Acceso Remoto (RAT) de varias etapas, llamado "ZuoRAT", y desarrollado para dispositivos SOHO, que permite que un agente se infiltre en la red local y acceda a sistemas adicionales en la LAN mediante la redirección de las comunicaciones red para mantener una presencia no detectada.

3. DETALLE:

El troyano RAT "ZuoRAT" es capaz de enumerar todos los dispositivos conectados al enrutador e infectarlos, capturar el tráfico de la red, realizar ataques Man-in-the-Middle (controlar DNS y HTTPS según reglas predefinidas), así como formas de permanecer desapercibido en el dispositivo. Para infectar dispositivos SOHO, el malware explota vulnerabilidades conocidas sin parches (CVE-2020-26878 y CVE-2020-26879).

Los investigadores señalan que algunos de los objetivos de ZuoRAT son los enrutadores de los fabricantes de marcas Cisco, Netgear, Asus y DrayTek, entre otros. La infección de los routers es utilizada como un vector de entrada para acceder a una red LAN y tomar el control total de los dispositivos conectados, que ejecuten sistemas con plataforma Windows, macOS y Linux.

A través del secuestro de DNS, las direcciones IP válidas que coinciden con el dominio se reemplazan por una IP maliciosa controlada por el atacante; y a través de la intrusión HTTP, se inyectan redireccionamientos 302 en la conexión para enviar al usuario a un sitio web malicioso controlado por un atacante. Utilizando estos dos métodos es posible instalar otros tipos de malware en los dispositivos conectados al enrutador comprometido. Asimismo, para infectar otro tipo de dispositivos, la campaña consta de al menos cuatro partes, tres de las cuales fueron desarrolladas y escritas desde cero:

- ZuoRAT, escrito para MIPS para routers
- Cbeacon RAT, escrito en C++ para Windows
- GoBeacon RAT, escrito en Go para dispositivos Linux y macOS
- Herramienta Cobalt Strike

Para evitar sospechas, el exploit de infección se descarga inicialmente desde un servidor privado virtual (VPS) dedicado que aloja el contenido malicioso. Luego, se aprovecha la comunicación entre los

enrutadores, se utilizan como proxy para acceder al servidor de comando y control (C2) y, finalmente, los enrutadores proxy se cambian periódicamente para dificultar la detección. La infraestructura de C2 se divide en dos conjuntos: uno para controlar los enrutadores infectados y otro dedicado a los dispositivos conectados que se infectarán más adelante.

4. RECOMENDACIONES:

- Bloquear los Indicadores de Compromiso (IoC) identificados de ZuoRAT (link aquí)
- La mayoría de los programas maliciosos para enrutadores SOHO no pueden sobrevivir a un reinicio del dispositivo afectado. El exploit inicial, que incluye archivos almacenados en la carpeta temporal, se elimina al reiniciar el dispositivo, y el proceso de recuperación completo requiere un restablecimiento de fábrica del dispositivo.

5. REFERENCIAS:

- https://blog.lumen.com/zuorat-hijacks-soho-routers-to-silently-stalk-networks/
- https://github.com/blacklotuslabs/IOCs/blob/main/ZuoRAT_IoCs.txt

Múltiples vulnerabilidades críticas en productos CISCO

Tipo de Ataque: **Explotación de vulnerabilidades conocidas**

Medio de Propagación: **Red, Internet**

1. **PRODUCTOS AFECTADOS:**

- Software Cisco Expressway Series y el software Cisco TelePresence VCS, versión 14.0 y anteriores (si están configuradas en la configuración por defecto)
- Cisco Smart Software Manager On-Prem y Cisco Smart Software Manager Satellite, versión 8 y anteriores

2. **RESUMEN:**

Cisco ha informado múltiples vulnerabilidades CRÍTICAS y de ALTA gravedad de tipo neutralización incorrecta de byte NULL o carácter NUL, recorrido de ruta absoluto y consumo de recursos descontrolado en algunos de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a los atacantes remotos sobrescribir archivos arbitrarios o realizar ataques de envenenamiento de bytes NULL y causar denegación de servicio (DoS) en un dispositivo afectado.

3. **DETALLE:**

La vulnerabilidad de sobreescritura de archivos arbitrarios CVE-2022-20812 en la API de la base de datos de encadenamiento de Cisco Expressway y Cisco TelePresence VCS podría permitir que un atacante remoto autenticado tenga permisos de lectura y escritura. El administrador escribe en la aplicación para realizar ataques transversales de ruta absolutos en el dispositivo afectado y sobrescribe los archivos del sistema operativo subyacente como usuario root.

La vulnerabilidad alta identificada como CVE-2022-20813 Cisco Expressway Series Null Byte Malicious Vulnerability y Cisco TelePresence VCS Certificate Validation podrían permitir que los atacantes remotos no autenticados obtengan una vulnerabilidad sensible al acceso no autorizado a los datos. Esta vulnerabilidad se debe a una validación de certificado incorrecta. Un atacante podría explotar esta vulnerabilidad mediante el uso de una técnica de intermediario para interceptar el tráfico entre dispositivos y luego usar un certificado diseñado para suplantar el punto final. Una explotación exitosa podría permitir a un atacante ver el tráfico interceptado en texto claro o modificar el contenido del tráfico.

Una vulnerabilidad de severidad alta identificada como CVE-2022-20808 en Cisco On-Prem Intelligent Software Manager (SSM On-Prem) podría permitir que un atacante remoto autenticado provoque la denegación de servicio en un dispositivo afectado. La vulnerabilidad se debe al mal manejo de múltiples registros de dispositivos simultáneos en Cisco SSM On-Prem. Un atacante podría aprovechar esta vulnerabilidad enviando múltiples solicitudes de registro de dispositivos a Cisco SSM On-Prem. Una explotación exitosa podría permitir que un atacante provoque una condición DoS en un dispositivo afectado.

Cisco indica que las vulnerabilidades son independientes entre sí. Explotar una de las vulnerabilidades no necesariamente requiere explotar otra. Además, una versión de software que se ve afectada por una de las vulnerabilidades de seguridad puede no verse afectada por las otras vulnerabilidades.

4. RECOMENDACIONES:

Se recomienda actualizar los productos afectados a una versión fija disponible que corrigen estas vulnerabilidades.

5. REFERENCIAS:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-expressway-overwrite-3buqW8LH
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/ciscosa-onprem-privesc-tP6uNZOS

Múltiples vulnerabilidades críticas en el controlador Festo CECC-X-M1

Tipo de Ataque: Explotación de vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. PRODUCTOS AFECTADOS:

- Controlador CECC-X-M1, versión 4.0.14, 3.8.14 y anteriores;

- Controlador CECC-X-M1-MV, versión 4.0.14, 3.8.14 y anteriores;

- Controlador CECC-X-M1-MV-S1, versión 4.0.14, 3.8.14 y anteriores;

- Controlador CECC-X-M1-YS-L1, Controlador CECC-X-M1-YS-L2, Controller CECC-X-M1-Y-YJKP, Kit de Servo Press YJKP y Kit de Servo Press YJKP, versión 3.8.14 y anteriores.

2. RESUMEN:

Investigadores del Laboratorio de Investigación ONEKEY han notificado a Festo sobre varias vulnerabilidades de inyección de comandos en diferentes versiones del controlador Festo CECC-X-M1 que podrían permitir ejecutar comandos arbitrarios del sistema como root.

3. DETALLE:

Los controladores Festo CECC-X-M1 en varias versiones se ven afectadas por vulnerabilidades de inyección de comandos sin necesidad de autenticación, mediante una petición tipo POST "cecc-x-web-viewer-request-off", lo que permitiría a un atacante obtener acceso al servidor web y ejecutar comandos arbitrarios del sistema. Se han asignado los identificadores CVE-2022-30308, CVE-2022-30309, CVE-2022-30310 y CVE-2022-30311 para estas vulnerabilidades.

Cabe señalar que cualquier persona que pueda obtener acceso al servidor web podría ejecutar comandos arbitrarios del sistema en el dispositivo con privilegios de root.

La vulnerabilidad de tipo Inyección de comando de sistema operativo se debe a que el software construye la totalidad o parte de un comando del sistema operativo utilizando la entrada influenciada externamente desde un componente ascendente, pero no neutraliza o neutraliza incorrectamente elementos especiales que podrían modificar el comando del sistema operativo previsto cuando se envía a un componente descendente.

4. RECOMENDACIONES:

Actualmente, Festo no ha identificado ninguna solución específica para esta vulnerabilidad. Como parte de una estrategia de seguridad, Festo recomienda las siguientes medidas generales de defensa para reducir el riesgo de exploits:

- Actualizar los productos afectados a la versión del firmware 3.8.18, 4.0.18 y/o superiores que corrigen estas vulnerabilidades
- Usar controladores y dispositivos solo en un entorno protegido para minimizar la exposición de la red y asegurarse de que no sean accesibles desde el exterior
- Usar firewalls para proteger y separar la red del sistema de control de otras redes

- Usar túneles VPN (redes privadas virtuales) si se requiere acceso remoto
- Activar y aplicar funciones de administración de usuarios y contraseñas
- Usar enlaces de comunicación encriptados
- Limitar el acceso tanto al sistema de desarrollo como al de control por medios físicos, características del sistema operativo, etc.
- Proteger tanto el sistema de desarrollo como el de control mediante el uso de soluciones de detección de virus actualizadas

5. REFERENCIAS:

- https://www.incibe-cert.es/alerta-temprana/avisos-sci/vulnerabilidad-inyeccion-comandos-festo-cecc-x-m1
- https://cert.vde.com/de/advisories/VDE-2022-020/

Nuevo malware Pipedream es dirigido a los Sistemas de Control Industriales (ICS)

Tipo de Ataque: Explotación de equipos en entornos de gas natural licuado (GNL) y energía eléctrica.

Medio de Propagación: Red, Internet

1. **PRODUCTOS AFECTADOS:**

- Controlador de máquina compacto: **Omron NX1P2 PLC**
- Controlador de seguridad: **Omron NX-SL3300**
- Controlador de automatización de máquinas: **Omron NJ501-1300 PLC**
- Acopladores EtherCAT: **Omron NX-ECC, NX-EIC202, NX-ECC203**
- Servoaccionamiento 1S: **Omron R88D1SN10F-ECT**
- Fuente de Alimentación: **Omron S8VK**
- Controlador lógico de borde nativo IIoT: **Schneider Modicon M241 (TM241)**
- Controlador lógico amigable: **Schneider Modicon M251 (TM251)**
- Controlador lógico/relé de E/S: **Schneider Modicon M221 (TM221)**
- Controlador lógico: **Schneider Modicon (TM238), Schneider Modicon M258 (TM258)**
- Controlador de movimiento: **Schneider LMC058, Schneider LMC078**

2. **RESUMEN:**

Pipedream es un nuevo malware específico de sistemas de control industrial (ICS), desarrollado por el grupo de amenazas Chernovite. Pipedream demuestra un importante componente de investigación y desarrollo centrado en la disrupción, la degradación y, potencialmente, la destrucción de entornos industriales y procesos físicos.

3. **DETALLE:**

Según Dragos Security, el malware Pipedream consta de una colección de componentes que puede afectar a una amplia variedad de controladores lógicos programables (PLC) y software industrial, incluidos los PLC específicos de Omron y Schneider Electric, y arquitectura unificada de comunicaciones de plataforma abierta mal configurada y servidores OPC-UA.

Uno de los PLC de Schneider Electric a los que apunta Pipedream, aprovecha CODESYS como su arquitectura de sistema subyacente debido a su falta de seguridad. CODESYS es un componente de software de terceros utilizado por cientos de fabricantes de equipos industriales. Si bien Pipedream actualmente puede identificar y apuntar a los PLC de Omron y Schneider Electric, sus herramientas pueden usarse para apuntar y atacar controladores de cientos de otros proveedores en múltiples verticales debido a su versatilidad.

Potencialmente, Pipedream podría utilizarse para ejecutar ataques contra las siguientes tecnologías industriales:

Modbus TCP: Es un protocolo de comunicación serie desarrollado y publicado por Modicon en 1979 para utilizar con sus PLC. En términos simples, es un método utilizado para transmitir información a través de una serie líneas entre dispositivos electrónicos. Modbus más tarde adoptó los protocolos de

comunicación TCP/IP para la Interconexión de Sistemas Abiertos (OSI) para expandir comunicaciones a través de redes interconectadas. El protocolo resultante ahora se denomina comúnmente como Modbus TCP y es uno de los protocolos ICS más comunes.

OPC-UA: La Arquitectura Unificada OPC (UA), lanzada en 2008, es una arquitectura orientada a servicios independientes de la plataforma que integra toda las especificaciones clásicas de las OPC (Open Platform Communication) en un marco extensible.

CODESYS: A través del sistema de control de runtime adaptable CODESYS, cualquier dispositivo inteligente se puede transformar en un controlador IEC 61131-3 completo. Actualmente es muy utilizado por varios fabricantes.

Windows: ASRock Motherboard Utility es una utilidad todo en uno diseñada para actualizaciones del sistema y descarga de software, integrada con una variedad de aplicaciones y software de soporte. ASRock Motherboard Utility proporciona las últimas actualizaciones de BIOS y software de actualización del sistema para que los usuarios las descarguen. ASRock Inc. es la tercera marca de placas madre más grande del mundo, y fabrica hardware y computadoras industriales y de consumo.

4. RECOMENDACIONES:

- **Mitigaciones tecnológicas de Schneider Electric**

Acción	Detalle
Cambiar las credenciales predeterminadas	Cuando sea factible, junto con el personal de operaciones y del sitio para PLC de la serie TM2xx de Schneider Electric: A partir del firmware 5.0, los dispositivos usan credenciales predeterminadas “Administrator/Administrator”, y estos deben cambiarse a un complejo contraseña utilizando el software EcoStruxure.
Restringir el acceso a UDP/1740-1743, TCP/1105 y TCP/11740	Para todos los PLC de la serie TM2xx de Schneider Electric.
Restringir el acceso a TCP/11740	Para los PLC que no son de Schneider que se sabe que se comunican con este puerto desde la estación de trabajo de ingeniería.
Deshabilitar Schneider NetManage servicio de descubrimiento	Junto con el personal de operaciones y del sitio, deshabilite Schneider Servicio de descubrimiento NetManage, ya que lo utiliza Chernovite para descubrir los PLC (ver VA-2019-02).
Supervisar los PLC afectados en busca de nuevos conexiones salientes	Busque comunicaciones con otros PLC en la red, en: UDP/1740-1743, TCP/1105 y TCP/11740.

Validar la ingeniería programas para estaciones de trabajo - Experto en máquinas EcoStruxure	Eliminar el software innecesario. Si es posible, aplicar la lista de permisos de la aplicación software en la estación de trabajo. Restringir la estación de trabajo para que no realice llamadas salientes conexiones de red, especialmente a servicios de Internet.

- **Mitigaciones de la tecnología Omron**

Acción	Detalle
Restringir el acceso a TCP/80, TCP/9600 y UDP/9600	Para todos los PLC de Omron. Solo permita que los sistemas EWS se comuniquen en estos puertos.
Validar la ingeniería de software para estaciones de trabajo – Omron Sysmac/CX-One/NX IO Configurador	Eliminar el software innecesario. Si es posible, aplicar la lista de permisos de la aplicación software en la estación de trabajo. Restringir la estación de trabajo para que no realice llamadas salientes conexiones de red, especialmente a servicios de Internet.

- **Mitigaciones OPC-UA**

Acción	Detalle
Habilitar la seguridad OPC-UA	Asegúrese de que la seguridad de OPC-UA esté configurada correctamente con la aplicación de autenticación habilitada y listas de confianza explícitas. Asegúrese de que las claves privadas del certificado y las contraseñas de usuario se almacenen de forma segura. Asegúrese de que mDNS (que transmite activamente la ubicación de los servidores OPC-UA) esté deshabilitado en todas las máquinas. Los operadores de ICS pueden gestionar la configuración de seguridad de sus dispositivos OPC-UA usando su software de estación de trabajo de ingeniería (en la mayoría de los casos). El uso del modo de seguridad de "solo inicio de sesión" con OPC-UA es óptimo para entornos ICS que aprovechan las soluciones de monitoreo de red. El modo de seguridad Signonly envía mensajes sin cifrar, pero con autenticación; código que permite a los receptores estar seguros de que el mensaje proviene de un remitente confiable.

	Esto protege contra herramientas como Mousehole que envían mensajes no autorizados a clientes y servidores OPC-UA mientras permite que los paquetes sean inspeccionados por dispositivos de seguridad de la red. Se pueden encontrar recomendaciones específicas para las mejores prácticas de seguridad de OPC-UA en la web de la fundación OPC-UA.

5. REFERENCIAS:

- https://hub.dragos.com/whitepaper/chernovite-pipedream
- https://opcfoundation.org/UA/Security/BestPractices.pdf