MITRE ATT&CK®

TÁCTICAS DE ICS PARA EXPLOITS DE OMRON

Lista de exploits

CJ2M-CPU31(Firmware)

Nombre	Vector de ataque	Tipo
CVE-2023-38744	Red	DoS
CVE-2023-27396	Red	Interceptar comunicaciones/Ejecutar comandos arbitrarios/Recuperar información del sistema
CVE-2022-45790	Red	Interceptar mensajes/Omitir la autenticación/Modificar valores

(No he encontrado más antiguos)

CJ2M(Hardware)

Nombre	Vector de ataque	Tipo
CVE-2015-1015	Local	Vulnerabilidad de contraseñas reversibles
CVE-2015-0987	Red	Transmisión insegura de contraseñas

CX-Programmer

Nombre	Vector de ataque	Tipo
CVE-2023-38748	Local	Corrupción de memoria/Filtración de información
CVE-2023-38747	Local	Desbordamiento/Corrupción de memoria/Filtración de información
CVE-2023-38746	Local	Filtración de información
CVE-2023-22317	Local	Corrupción de memoria/Filtración de información
CVE-2023-22314	Local	Corrupción de memoria/Filtración de información
CVE-2023-22277	Local	Corrupción de memoria/Filtración de información
CVE-2022-43667	Local	Desbordamiento/Corrupción de memoria/Filtración de información
CVE-2022-43509	Local	Corrupción de memoria/Filtración de información
CVE-2022-43508	Local	Corrupción de memoria/Filtración de información
CVE-2022-25325	Local/Red	Corrupción de memoria/Filtración de información
CVE-2022-25234	Local/Red	Corrupción de memoria/Filtración de información
CVE-2022-25230	Local/Red	Corrupción de memoria/Filtración de información
CVE-2022-21219	Local/Red	Filtración de información
CVE-2022-21124	Local/Red	Corrupción de memoria/Filtración de información
CVE-2022-3398	Local/Red	Corrupción de memoria/Ejecutar código
CVE-2022-3397	Local/Red	Corrupción de memoria/Ejecutar código

CVE-2022-3396	Local/Red	Corrupción de memoria/Ejecutar código
CVE-2022-2979	Local/Local	Corrupción de memoria
CVE-2019-6556	Local/Red	Ejecutar código
CVE-2018-18993	Local/Red	Desbordamiento/Corrupción de memoria/Ejecutar código
CVE-2018-18989	Local/Red	Ejecutar código
CVE-2018-8834	Local/Local	Desbordamiento/Corrupción de memoria
CVE-2018-7514	Local/Local	Desbordamiento/Corrupción de memoria

(Los que son de doble vector es que se puede utilizar de una manera o de otra)

Táctica de cada exploit

CVE-ID: CVE-2023-38744

Descripción:

Vulnerabilidad de denegación de servicio (DoS) debido a la validación inadecuada de un tipo especificado de entrada en el puerto EtherNet/IP integrado de la unidad de CPU CJ Series CJ2 y la función de comunicación de la unidad EtherNet/IP CS/CJ Series. Si un producto afectado recibe un paquete especialmente diseñado por un atacante remoto no autenticado, la unidad del producto afectado puede caer en una condición de denegación de servicio (DoS). Los productos/versiones afectados son los siguientes: Unidad de CPU CJ2M CJ2M-CPU3[] versión de la sección EtherNet/IP integrada Ver. 2.18 y anteriores, Unidad de CPU CJ2H CJ2H-CPU6[]-EIP versión de la sección EtherNet/IP integrada Ver. 3.04 y anteriores, Unidad EtherNet/IP CS/CJ Series CS1W-EIP21 V3.04 y anteriores, y Unidad EtherNet/IP CS/CJ Series CJ1W-EIP21 V3.04 y anteriores.

Tipo de vulnerabilidad:

CVE-2023-38744 (Denegacion de servicios)

Comportamientos de adversario de MITRE ATT&CK:

CVE-2023-38744 > PERMITE > T1499 (Denegación de servicios) > HABILITA > T1071 (Protocolo de Capa de Aplicación) > CONDUCE A > T1059 (Interfaz de Línea de Comandos)

CVE-ID: CVE-2023-27396

Descripción:

El protocolo de comunicación de mensajes FINS (Factory Interface Network Service) está diseñado para ser utilizado en redes FA (Automatización de Fábricas) cerradas, y se utiliza en redes FA compuestas por productos de OMRON. Múltiples productos de OMRON que implementan el protocolo FINS contienen los siguientes problemas de seguridad: (1) Comunicación en texto plano y (2) No se requiere autenticación. Cuando se interceptan los mensajes FINS, se pueden recuperar los contenidos. Cuando se inyectan mensajes FINS arbitrarios, se pueden ejecutar cualquier

comando en el dispositivo afectado o se puede recuperar la información del sistema. Los productos y versiones afectados son los siguientes: Unidades de CPU de la serie SYSMAC CS, todas las versiones; Unidades de CPU de la serie SYSMAC CJ, todas las versiones; Unidades de CPU de la serie SYSMAC CP, todas las versiones; Unidades de CPU de la serie SYSMAC NJ, todas las versiones; Unidades de CPU de la serie SYSMAC NX1P, todas las versiones; Unidades de CPU de la serie SYSMAC NX102, todas las versiones; y Unidades de CPU de conexión a base de datos SYSMAC NX7 (Ver.1.16 o posterior).

Tipo de vulnerabilidad:

CVE-2023-27396 (Comunicación en texto plano, No se requiere autenticación)

Comportamientos de adversario de MITRE ATT&CK:

CVE-2023-27396 > PERMITE > T1041 (Credenciales en texto plano) > HABILITA > T1569 (Descubrimiento de Información del Sistema) > CONDUCE A > T1059 (Interfaz de Línea de Comandos)

CVE-ID: CVE-2022-45790

Descripción:

El protocolo Omron FINS tiene una característica de autenticación para evitar el acceso a regiones de memoria. La autenticación es susceptible a ataques de fuerza bruta, lo que puede permitir que un adversario obtenga acceso a la memoria protegida. Este acceso puede permitir la sobrescritura de valores, incluida la lógica programada.

Tipo de vulnerabilidad:

CVE-2022-45790 (Autenticación Susceptible a Ataques de Fuerza Bruta)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-45790 > PERMITE > T1110 (Fuerza Bruta) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1047 (Instrumentación de Administración de Windows)

CVE-ID: CVE-2015-1015

Descripción:

Omron CX-One CX-Programmer antes de la versión 9.6, dispositivos PLC CJ2M antes de la versión 2.1 y dispositivos PLC CJ2H antes de la versión 1.5 utilizan un formato reversible para el almacenamiento de contraseñas en archivos de objetos en tarjetas Compact Flash, lo que facilita a los usuarios locales obtener información sensible mediante la lectura de un archivo.

Tipo de vulnerabilidad:

CVE-2015-1015 (Almacenamiento de Contraseñas en Formato Reversible)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2015-1015 > PERMITE > T1552 (Credenciales no seguras) > HABILITA > T1003 (Extracción de Credenciales) > CONDUCE A > T1059 (Interfaz de Línea de Comandos)

CVE-ID: CVE-2015-0987

Descripción:

Omron CX-One CX-Programmer antes de la versión 9.6, dispositivos PLC CJ2M antes de la versión 2.1 y dispositivos PLC CJ2H antes de la versión 1.5 dependen de la transmisión de contraseñas en texto claro, lo que permite que atacantes remotos obtengan información sensible al husmear en la red durante una solicitud de desbloqueo del PLC.

Tipo de vulnerabilidad:

CVE-2015-0987 (Transmisión de Contraseñas en Texto Claro)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2015-0987 > PERMITE > T1569 (Descubrimiento de Información del Sistema) > HABILITA > T1040 (Intercepción de Red) > CONDUCE A > T1059 (Interfaz de Línea de Comandos)

CVE-ID: CVE-2023-38748

Descripción:

Existe una vulnerabilidad de uso después de liberar (Use after free) en CX-Programmer incluido en CX-One CXONE-AL[][]D-V4 V9.80 y versiones anteriores. Al hacer que un usuario abra un archivo CXP especialmente diseñado, puede ocurrir una divulgación de información y/o ejecución de código arbitrario.

Tipo de vulnerabilidad:

CVE-2023-38748 (Uso Después de Liberar)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2023-38748 > PERMITE > T1059 (Interfaz de Línea de Comandos) > HABILITA > T1560 (Archivar Datos Recopilados) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2023-38747

Descripción:

Existe una vulnerabilidad de desbordamiento de búfer basado en el montículo (Heap-based buffer overflow) en CX-Programmer incluido en CX-One CXONE-AL[][]D-V4 V9.80 y versiones anteriores. Al hacer que un usuario abra un archivo CXP especialmente diseñado, puede ocurrir una divulgación de información y/o ejecución de código arbitrario.

Tipo de vulnerabilidad:

CVE-2023-38747 (Desbordamiento de Búfer Basado en el Montículo)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2023-38747 > PERMITE > T1192 (Ejecución de Proxy de Binario Firmado) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1569 (Descubrimiento de Información del Sistema)

CVE-ID: CVE-2023-38746

Descripción:

Existe una vulnerabilidad de lectura fuera de límites (Out-of-bounds read) en CX-Programmer incluido en CX-One CXONE-AL[][]D-V4 V9.80 y versiones anteriores. Al hacer que un usuario abra un archivo CXP especialmente diseñado, puede ocurrir una divulgación de información y/o ejecución de código arbitrario.

Tipo de vulnerabilidad:

CVE-2023-38746 (Lectura Fuera de Límites)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2023-38746 > PERMITE > T1552 (Credenciales no seguras) > HABILITA > T1560 (Archivar Datos Recopilados) > CONDUCE A > T1059 (Interfaz de Línea de Comandos)

CVE-ID: CVE-2023-22317

Descripción:

Existe una vulnerabilidad de uso después de liberar (Use after free) en CX-Programmer Ver.9.79 y versiones anteriores. Al hacer que un usuario abra un archivo CXP especialmente diseñado, puede

ocurrir una divulgación de información y/o ejecución de código arbitrario. Esta vulnerabilidad es distinta de CVE-2023-22277 y CVE-2023-22314.

Tipo de vulnerabilidad:

CVE-2023-22317 (Uso Después de Liberar)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2023-22317 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2023-22317

Descripción:

Existe una vulnerabilidad de uso después de liberar (Use after free) en CX-Programmer Ver.9.79 y versiones anteriores. Al hacer que un usuario abra un archivo CXP especialmente diseñado, puede ocurrir una divulgación de información y/o ejecución de código arbitrario. Esta vulnerabilidad es distinta de CVE-2023-22277 y CVE-2023-22314.

Tipo de vulnerabilidad:

CVE-2023-22317 (Uso Después de Liberar)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2023-22317 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2023-22277

Descripción:

Existe una vulnerabilidad de uso después de liberar (Use after free) en CX-Programmer Ver.9.79 y versiones anteriores. Al hacer que un usuario abra un archivo CXP especialmente diseñado, puede ocurrir una divulgación de información y/o ejecución de código arbitrario. Esta vulnerabilidad es distinta de CVE-2023-22317 y CVE-2023-22314.

Tipo de vulnerabilidad:

CVE-2023-22277 (Uso Después de Liberar)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2023-22277 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2022-43667

Descripción:

Existe una vulnerabilidad de desbordamiento de búfer basado en la pila (Stack-based buffer overflow) en CX-Programmer v.9.77 y versiones anteriores, lo que puede llevar a la divulgación de información y/o ejecución de código arbitrario al hacer que un usuario abra un archivo CXP especialmente diseñado.

Tipo de vulnerabilidad:

CVE-2022-43667 (Desbordamiento de Búfer Basado en la Pila)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-43667 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2022-43509

Descripción:

Existe una vulnerabilidad de escritura fuera de límites (Out-of-bounds write) en CX-Programmer v.9.77 y versiones anteriores, lo que puede llevar a la divulgación de información y/o ejecución de código arbitrario al hacer que un usuario abra un archivo CXP especialmente diseñado.

Tipo de vulnerabilidad:

CVE-2022-43509 (Escritura Fuera de Límites)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-43509 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2022-43508

Descripción:

Existe una vulnerabilidad de uso después de liberar (Use-after free) en CX-Programmer v.9.77 y versiones anteriores, lo que puede llevar a la divulgación de información y/o ejecución de código arbitrario al hacer que un usuario abra un archivo CXP especialmente diseñado.

Tipo de vulnerabilidad:

CVE-2022-43508 (Uso Después de Liberar)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-43508 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2022-25325

Descripción:

Existe una vulnerabilidad de uso después de liberar (Use after free) en CX-Programmer v9.76.1 y versiones anteriores, que forma parte del conjunto CX-One (v4.60). Esto permite que un atacante cause la divulgación de información y/o la ejecución de código arbitrario al hacer que un usuario abra un archivo CXP especialmente diseñado. Esta vulnerabilidad es distinta de CVE-2022-25230.

Tipo de vulnerabilidad:

CVE-2022-25325 (Uso Después de Liberar)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-25325 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2022-25234

Descripción:

Existe una vulnerabilidad de escritura fuera de límites (Out-of-bounds write) en CX-Programmer v9.76.1 y versiones anteriores, que forma parte del conjunto CX-One (v4.60). Esto permite que un atacante cause la divulgación de información y/o la ejecución de código arbitrario al hacer que un usuario abra un archivo CXP especialmente diseñado. Esta vulnerabilidad es distinta de CVE-2022-21124.

Tipo de vulnerabilidad:

CVE-2022-25234 (Escritura Fuera de Límites)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-25234 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2022-25230

Descripción:

Existe una vulnerabilidad de uso después de liberar (Use after free) en CX-Programmer v9.76.1 y versiones anteriores, que forma parte del conjunto CX-One (v4.60). Esto permite que un atacante cause la divulgación de información y/o la ejecución de código arbitrario al hacer que un usuario abra un archivo CXP especialmente diseñado. Esta vulnerabilidad es distinta de CVE-2022-25325.

Tipo de vulnerabilidad:

CVE-2022-25230 (Uso Después de Liberar)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-25230 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2022-21219

Descripción:

Existe una vulnerabilidad de lectura fuera de límites (Out-of-bounds read) en CX-Programmer v9.76.1 y versiones anteriores, que forma parte del conjunto CX-One (v4.60). Esto permite que un atacante cause la divulgación de información y/o la ejecución de código arbitrario al hacer que un usuario abra un archivo CXP especialmente diseñado.

Tipo de vulnerabilidad:

CVE-2022-21219 (Lectura Fuera de Límites)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-21219 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2022-21124

Descripción:

Existe una vulnerabilidad de escritura fuera de límites (Out-of-bounds write) en CX-Programmer v9.76.1 y versiones anteriores, que forma parte del conjunto CX-One (v4.60). Esto permite que un atacante cause la divulgación de información y/o la ejecución de código arbitrario al hacer que un usuario abra un archivo CXP especialmente diseñado. Esta vulnerabilidad es distinta de CVE-2022-25234.

Tipo de vulnerabilidad:

CVE-2022-21124 (Escritura Fuera de Límites)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-21124 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2022-3398

Descripción:

OMRON CX-Programmer 9.78 y versiones anteriores son vulnerables a una escritura fuera de límites (Out-of-Bounds Write), lo que puede permitir que un atacante ejecute código arbitrario.

Tipo de vulnerabilidad:

CVE-2022-3398 (Escritura Fuera de Límites)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-3398 > PERMITE > T1059 (Interfaz de Línea de Comandos) > HABILITA > T1560 (Archivar Datos Recopilados) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2022-3397

Descripción:

OMRON CX-Programmer 9.78 y versiones anteriores son vulnerables a una escritura fuera de límites (Out-of-Bounds Write), lo que puede permitir que un atacante ejecute código arbitrario.

Tipo de vulnerabilidad:

CVE-2022-3397 (Escritura Fuera de Límites)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-3397 > PERMITE > T1059 (Interfaz de Línea de Comandos) > HABILITA > T1560 (Archivar Datos Recopilados) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2022-3396

Descripción:

OMRON CX-Programmer 9.78 y versiones anteriores son vulnerables a una escritura fuera de límites (Out-of-Bounds Write), lo que puede permitir que un atacante ejecute código arbitrario.

Tipo de vulnerabilidad:

CVE-2022-3396 (Escritura Fuera de Límites)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-3396 > PERMITE > T1059 (Interfaz de Línea de Comandos) > HABILITA > T1560 (Archivar Datos Recopilados) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2022-2979

Descripción:

Abrir un archivo especialmente diseñado podría hacer que el producto afectado no libere su referencia de memoria, lo que podría resultar en la ejecución arbitraria de código.

Tipo de vulnerabilidad:

CVE-2022-2979 (Fallo al Liberar la Referencia de Memoria)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2022-2979 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2019-6556

Descripción: Cuando se procesan archivos de proyecto, la aplicación (Omron CX-Programmer v9.70 y versiones anteriores y Componentes Comunes de enero de 2019 y anteriores) no verifica si está haciendo referencia a memoria liberada. Un atacante podría utilizar un archivo de proyecto especialmente diseñado para explotar y ejecutar código bajo los privilegios de la aplicación.

Tipo de vulnerabilidad:

CVE-2019-6556 (Fallo al Verificar Referencia de Memoria Liberada)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2019-6556 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2018-18993

Descripción:

Se han descubierto dos vulnerabilidades de desbordamiento de búfer basado en la pila en CX-One versiones 4.42 y anteriores (CX-Programmer versiones 9.66 y anteriores y CX-Server versiones 5.0.23 y anteriores). Cuando se procesan archivos de proyecto, la aplicación permite que los datos de entrada excedan el búfer. Un atacante podría utilizar un archivo de proyecto especialmente diseñado para desbordar el búfer y ejecutar código bajo los privilegios de la aplicación.

Tipo de vulnerabilidad:

CVE-2018-18993 (Desbordamiento de Búfer Basado en la Pila)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2018-18993 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2018-18989

Descripción:

En CX-One versiones 4.42 y anteriores (CX-Programmer versiones 9.66 y anteriores y CX-Server versiones 5.0.23 y anteriores), al procesar archivos de proyecto, la aplicación no verifica si está haciendo referencia a memoria liberada. Un atacante podría utilizar un archivo de proyecto especialmente diseñado para explotar y ejecutar código bajo los privilegios de la aplicación.

Tipo de vulnerabilidad:

CVE-2018-18989 (Fallo al Verificar Referencia de Memoria Liberada)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2018-18989 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2018-8834

Descripción:

El análisis de archivos de proyecto malformados en Omron CX-One versiones 4.42 y anteriores, incluyendo las siguientes aplicaciones: CX-FLnet versiones 1.00 y anteriores, CX-Protocol versiones 1.992 y anteriores, CX-Programmer versiones 9.65 y anteriores, CX-Server versiones 5.0.22 y anteriores, Network Configurator versiones 3.63 y anteriores, y Switch Box Utility versiones 1.68 y anteriores, puede causar un desbordamiento de búfer basado en el montículo (heap-based buffer overflow).

Tipo de vulnerabilidad:

CVE-2018-8834 (Desbordamiento de Búfer Basado en el Montículo)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2018-8834 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

CVE-ID: CVE-2018-7514

Descripción:

El análisis de archivos de proyecto malformados en Omron CX-One versiones 4.42 y anteriores, incluyendo las siguientes aplicaciones: CX-FLnet versiones 1.00 y anteriores, CX-Protocol versiones 1.992 y anteriores, CX-Programmer versiones 9.65 y anteriores, CX-Server versiones 5.0.22 y anteriores, Network Configurator versiones 3.63 y anteriores, y Switch Box Utility versiones 1.68 y anteriores, puede causar un desbordamiento de búfer basado en la pila (stack-based buffer overflow).

Tipo de vulnerabilidad:

CVE-2018-7514 (Desbordamiento de Búfer Basado en la Pila)

Comportamientos del adversario de MITRE ATT&CK:

CVE-2018-7514 > PERMITE > T1560 (Archivar Datos Recopilados) > HABILITA > T1059 (Interfaz de Línea de Comandos) > CONDUCE A > T1552 (Credenciales no seguras)

BIBLIOGRAFIA

https://attack.mitre.org/tactics/ics/
https://www.cvedetails.com/vulnerability-list/vendor_id-527/Omron.html