Boletín de Ciberseguridad

Riesgo de Ransomware y Vulnerabilidades Industriales

09-Jun-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

Los últimos ataques del Grupo Conti, tanto en Costa Rica como en Perú, están amenazando también a la seguridad de las empresas locales. La Asociación de Bancos del Perú (ASBANC) emitió un comunicado indicando que la brecha de información de datos personales al Estado Peruano compromete la autenticación segura de los usuarios a todo nivel, no solo la requerida para transacciones en las instituciones bancarias, sino también para virtualmente todas las plataformas digitales.

Este panorama aumenta significativamente el riesgo latente de enfrentar amenazas de Ransomware. Fabricantes como Microsoft y QNAP han publicado actualizaciones de Día Cero y de urgencia para eliminar vulnerabilidades existentes que facilitaban el éxito de estos ataques.

Por otro lado, este mes se han detectado nuevas vulnerabilidades de severidad crítica y alta en sistemas industriales de Cambium Networks y Mitsubishi Electrics, amenazando la integridad y disponibilidad de las redes industriales con este tipo de activos o sistemas.

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

Nombre de la alerta:

Ransomware Conti presume atacar servicios críticos de Perú

Tipo de Ataque: Ransomware

Medio de Propagación: USB, Disco, Red, Correo, Navegación de Internet

1. Datos Generales:

El grupo ruso que se especializa en vulnerar plataformas públicas, secuestrando datos y sistemas, obligó a declarar el Estado de Emergencia en Costa Rica. Expertos advierten que este puede ser sólo uno de muchos otros ataques a entidades oficiales de países como Perú, Chile y México, entre otros.

2. Tema:

Se presume que los ciberdelincuentes usan malware como Trickbot y Emotet para el acceso inicial a una organización. La defensa contra estos ataques se complica por la presencia de errores humanos. Cuando un solo empleado hace clic en un enlace malicioso, toda la infraestructura crítica de una organización puede verse comprometida.

"Obtendrán credenciales adicionales. Pueden leer mensajes de correos electrónicos y conversaciones privadas de cualquier empresa. Solo se necesita una vulnerabilidad para que todo quede expuesto", señala Steph Shample, experta en ciberseguridad y asociada al Instituto de Oriente Medio.

En medio de ataques de Ransomware a gran escala en Costa Rica y Perú, supuestamente ambos ejecutados por la infame banda de Ransomware Conti, el Departamento de Estado de EEUU emitió un comunicado el 6 de mayo ofreciendo una recompensa de hasta US$ 10 millones por información que conduzca a la identificación o ubicación de personas involucradas.

La banda de ciberdelincuentes presume desde la Deep web ser una amenaza para los servicios críticos de Perú, incluido el servicio de agua y de electricidad.

3. Conclusión:

De acuerdo con el portavoz del Departamento de Estado, Ned Price, el FBI estima que más de 1.000 víctimas del grupo Conti han pagado un total de más de US$ 150 millones en pagos de Ransomware.

En los primeros cuatro meses del 2022, Check Point Research (CPR), informó que, en promedio, una de cada 60 organizaciones en todo el mundo se ha visto afectada por un intento de ataque de ransomware cada semana, un aumento interanual del 14%.

4. Recomendación:

- Concientizar al equipo de trabajo en todos los niveles de la institución.
- Contar con directrices de respaldo y protección de datos.
- Contar con directrices vigentes de autenticación multifactor en los sistemas de información.
- Contar con soluciones de ciberseguridad vigentes y actualizadas.
- Contar con un plan de respuesta ante incidentes.

5. Referencia:

❖ https://10news.org/2022/05/conti-amenaza-con-cortar-el-agua-y-la-luz/

Nombre de la alerta:

CVE-2022-30190 Vulnerabilidad de Día Cero en Microsoft

Tipo de Ataque: **Vulnerabilidad de ejecución remota de código**

Medio de Propagación: **Archivos Word, Micorsoft Support Diagnostic Tool (MSDT)**

1. **Productos Afectados:**

La vulnerabilidad afecta el protocolo URL del Microsoft Support Diagnostic Tool (MSDT), existente en Windows Server 2019, Windows 10 versión 1809 y versiones posteriores.

2. **Resumen:**

Existe una vulnerabilidad de ejecución de código en remoto cuando se llama a MSDT mediante el protocolo URL desde una aplicación de llamada como Word.

3. **Detalles:**

Un atacante que aproveche con éxito esta vulnerabilidad puede ejecutar código arbitrario con los privilegios de la aplicación que realiza la llamada. Luego, el atacante puede instalar programas, ver, cambiar o eliminar datos, o crear nuevas cuentas en el contexto permitido por los derechos del usuario.

4. **Solución:**
   - Deshabilitar temporalmente el protocolo URL del MSDT, lo que previene que los *troubleshooters* se inicien como enlaces, incluidos enlaces en todo el sistema operativo. Con la deshabilitación, los *troubleshooters* igual pueden ser accedidos mediante la aplicación Get Help o en configuración de sistemas.

5. **Referencia:**
   - Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability – Microsoft Security Response Center

Nombre de la alerta:

Vulnerabilidad de omisión de restricciones de seguridad en PostgreSQL

Tipo de Ataque: Explotación de vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. Productos Afectados:

PostgreSQL versión:

- 10.20 y anteriores;
- 11.15 y anteriores;
- 12.10 y anteriores;
- 13.6 y anteriores;
- 14.2 y anteriores.

2.Resumen:

Se ha reportado una vulnerabilidad de severidad MEDIA de tipo permisos, privilegios y controles de acceso en múltiples versiones de PostgreSQL. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado eludir las restricciones de seguridad implementadas y escalar privilegios dentro de la aplicación.

3. Detalles:

- La vulnerabilidad de permisos, privilegios y controles de acceso en múltiples versiones de PostgreSQL se debe a que los puntos débiles de esta categoría están relacionados con la gestión de permisos, privilegios y otras características de seguridad que se utilizan para realizar el control de acceso.
- La vulnerabilidad identificada como CVE-2022-1552 podría permitir a un usuario remoto eludir las restricciones de seguridad implementadas. La vulnerabilidad existe debido a restricciones de seguridad impuestas incorrectamente en Autovacuum, REINDEX, CREATE INDEX, REFRESH MATERIALIZED VIEW, CLUSTER y pg_amcheck. Un usuario remoto autenticado con permiso para crear objetos no temporales puede ejecutar funciones SQL arbitrarias bajo una identidad de super-usuario y escalar privilegios dentro de la aplicación.
- Un atacante tendría que enviar una solicitud especialmente diseñada a la aplicación afectada para aprovechar esta vulnerabilidad.

4. Solución:

Se recomienda actualizar PostgreSQL a la versión: 10.21, 11.16, 12.11, 13.7 o 14.3.

5. Referencia:

- https://www.postgresql.org/about/news/postgresql-143-137-1211-1116-and-1021-released-2449/

Nombre de la alerta:

Vulnerabilidad en el software de Cisco IOS XE para los switches de la familia Cisco Catalyst 9000 y los controladores inalámbricos de la familia Cisco Catalyst 9000

Tipo de Ataque: Explotación de vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. Productos Afectados:

Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco IOS XE para los switches de la familia Cisco Catalyst 9000 o los controladores inalámbricos de la familia Cisco Catalyst 9000:

- Switches de la serie Catalyst 9300;
- Switches de la serie Catalyst 9400;
- Switches de la serie Catalyst 9500;
- Switches de la serie Catalyst 9600;
- Controladores inalámbricos integrados Catalyst 9800 para switches de las series Catalyst 9300, 9400 y 9500;
- Controladores inalámbricos de la serie Catalyst 9800;
- Controladores inalámbricos Catalyst 9800-CL para la nube;
- Controladores inalámbricos integrados en puntos de acceso Catalyst.

2. Resumen:

Cisco ha reportado una vulnerabilidad de severidad ALTA de tipo asignación de privilegios incorrecta que afecta al software Cisco IOS XE para los switches de la familia Cisco Catalyst 9000 y los controladores inalámbricos de la familia Cisco Catalyst 9000 de Cisco. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario local autenticado elevar privilegios en un dispositivo afectado.

3. Detalles:

- La vulnerabilidad de tipo asignación de privilegios incorrecta se debe a que el producto afectado asigna incorrectamente un privilegio a un actor en particular, creando una esfera de control no deseada para ese actor. Un usuario puede acceder a funciones restringidas y/o información confidencial que puede incluir funciones administrativas y cuentas de usuario.
- La vulnerabilidad identificada como CVE-2022-20681 en la CLI del software Cisco IOS XE para los switches de la familia Cisco Catalyst 9000 y los controladores inalámbricos de la familia Cisco Catalyst 9000 podría permitir que un atacante local autenticado eleve los privilegios al nivel 15 en un dispositivo afectado.
- Esta vulnerabilidad se debe a una validación insuficiente de los privilegios del usuario después de que el usuario ejecuta ciertos comandos CLI. Un atacante podría aprovechar esta vulnerabilidad iniciando sesión en un dispositivo afectado como un usuario con privilegios bajos y luego ejecutando ciertos comandos CLI. Una explotación exitosa podría permitir que el atacante ejecute comandos arbitrarios con privilegios de nivel 15 en el dispositivo afectado.

4. Solución:

Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad.

5. Referencias:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlcpriv-esc-ybvHKO5

Nombre de la alerta:

Múltiples vulnerabilidades críticas en el sistema de gestión de red cnMaestro de Cambium Networks

Tipo de Ataque: Explotación de vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. **Productos Afectados:**
   - cnMaestro On-Premises: todas las versiones anteriores a 3.0.3-r32.
   - cnMaestro On-Premises: todas las versiones anteriores a 2.4.2-r29.
   - cnMaestro On-Premises: todas las versiones anteriores a 3.0.0-r34.

2. **Resumen:**
   El investigador, Noam Moshe de Claroty, ha reportado múltiples vulnerabilidades de severidad CRÍTICA y ALTA de tipo inyección de comandos del SO, inyección de SQL, travesía de rutas y uso de funciones potencialmente peligrosas en el sistema de gestión de red "cnMaestro" de Cambium Networks. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante la ejecución remota de código, la filtración de datos confidenciales y la toma completa de la infraestructura principal de la nube multi-tenant (multi-inquilino).

3. **Detalles:**
   - La vulnerabilidad de severidad crítica identificada como **CVE-2022-1357** de inyección de comando de sistema operativo, podría permitir a un atacante no autenticado acceder al servidor cnMaestro y ejecutar código arbitrario con los privilegios del servidor web. Esta falta de validación podría permitir a un atacante agregar datos arbitrarios al comando del registrador.

   - La vulnerabilidad de severidad alta identificada como **CVE-2022-1361** de inyección de SQL en cnMaestro On-Premises, se debe a una filtración de datos previa a la autenticación a través de la neutralización incorrecta de elementos especiales utilizados en un comando SQL. Esto podría permitir a un atacante filtrar datos sobre las cuentas y dispositivos de otros usuarios.

   - La vulnerabilidad de severidad alta identificada como **CVE-2022-1360** de inyección de comando de sistema operativo en cnMaestro On-Premises es vulnerable a la ejecución de código en el servidor de alojamiento cnMaestro. Esto podría permitir a un atacante remoto cambiar los ajustes de configuración del servidor.

   - La vulnerabilidad de severidad alta identificada como CVE-2022-1356 de uso de la función potencialmente peligrosa en cnMaestro On-Premises es vulnerable a una escalada de privilegios local. De forma predeterminada, un usuario no tiene privilegios de root. Sin embargo, un usuario puede ejecutar secuencias de comandos como "sudo", lo que podría permitir a un atacante obtener privilegios de root al ejecutar secuencias de comandos de usuario fuera de los comandos permitidos.

- Para las vulnerabilidades de severidad media se han asignado los siguientes identificadores: **CVE-2022-1358**, **CVE-2022-1359** y **CVE-2022-1362**.

4. Solución:

Cambium Networks recomienda aplicar uno de los siguientes paquetes de actualización:

- 3.0.3-r32;
- 2.4.2-r29;
- 3.0.0-r34;

Para los usuarios de cnMaestro Cloud, estas vulnerabilidades han sido parchadas por Cambium Networks y no se requiere ninguna otra acción.

5. Referencias:

- **https://nvd.nist.gov/vuln/detail/CVE-2022-1357**
- **https://nvd.nist.gov/vuln/detail/CVE-2022-1361**
- **https://nvd.nist.gov/vuln/detail/CVE-2022-1360**
- **https://nvd.nist.gov/vuln/detail/CVE-2022-1356**
- **https://nvd.nist.gov/vuln/detail/CVE-2022-1358**
- **https://nvd.nist.gov/vuln/detail/CVE-2022-1359**
- **https://nvd.nist.gov/vuln/detail/CVE-2022-1362**
- **https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-04**

Nombre de la alerta:

Múltiples vulnerabilidades en varios productos de la Serie MELSEC iQ-F de Mitsubishi Electric

Tipo de Ataque: Explotación de vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. Productos Afectados:

Las siguientes versiones del módulo de CPU de la serie iQ-F de MELSEC se ven afectadas:

- MELSEC iQ-F FX5U-xM y/zx=32,64,80, y=T,R, z=ES,DS,ESS,DSS: Todas las versiones anteriores a 1.270.
- MELSEC iQ-F FX5UC-x My/zx=32,64,96, y=T,R, z=D,DSS: Todas las versiones anteriores a 1.270.
- MELSEC iQ-F FX5UC-32 MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS: Todas las versiones anteriores a 1.270.
- MELSEC iQ-F FX5UJ-x My/zx=24,40,60, y=T,R, z=ES,ESS: Todas las versiones anteriores a 1.030.

2. Resumen:

Anton Dorfman de Positive Technologies, ha reportado dos vulnerabilidades de severidad ALTA de tipo validación de entrada incorrecta en diversas versiones del módulo de CPU de la serie iQ-F de MELSEC de Mitsubishi Electric. La explotación exitosa de estas vulnerabilidades podría causar una condición de denegación de servicio mediante el envío de paquetes especialmente diseñados. Se requiere un reinicio del sistema para la recuperación.

3. Detalles:

- La vulnerabilidad de validación de entrada incorrecta se debe a que el producto recibe entradas o datos, pero no valida o valida incorrectamente que la entrada tiene las propiedades necesarias para procesar los datos de forma segura y correcta. La validación de entrada es una técnica utilizada con frecuencia para verificar entradas potencialmente peligrosas con el fin de garantizar que las entradas sean seguras para el procesamiento dentro del código o cuando se comunican con otros componentes. Cuando el software no valida la entrada correctamente, un atacante puede crear la entrada en un formulario que no espera el resto de la aplicación. Esto llevará a que partes del sistema reciban entradas no deseadas, lo que puede resultar en un flujo de control alterado, control arbitrario de un recurso o ejecución de código arbitrario.
- Las vulnerabilidades de severidad alta identificadas como **CVE-2022-25161** y **CVE-2022-25162** de validación de entrada incorrecta en los productos afectados, son vulnerables a un paquete especialmente diseñado, lo que puede permitir que un atacante provoque una condición de denegación de servicio en la que se requiera un reinicio del sistema para la recuperación.
- Los sectores de infraestructuras críticas de fabricación en todo el mundo se ven afectadas.

4. Solución:

Mitsubishi Electric recomienda actualizar los productos afectados a las siguientes versiones disponibles que corrigen estas vulnerabilidades:

- FX5U-xMy/zx=32,64,8, y=T,R, z=ES,DS,ESS,DSS con número de serie 17X**** o posterior actualizado a v1.270 o posterior
- FX5UC-xMy/zx=32,64,96, y=T,R, z=D,DSS con número de serie 17X**** o posterior actualización a v1.270 o posterior
- Actualización de FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS a v1.270 o posterior;
- FX5UJ-xMy/zx=24,40,6 0, y=T,R, z=ES,ESS actualización a v1.030 o posterior.

Asimismo, Mitsubishi Electric recomienda aplicar las siguientes mitigaciones o soluciones alternativas:

- Utilizar un firewall o una red privada virtual para evitar el acceso no autorizado cuando se requiera acceso a Internet.
- Utilizar un firewall o una función de filtro de IP para restringir las conexiones a estos productos y evitar el acceso desde redes o hosts que no sean de confianza. Para obtener detalles sobre la función de filtro de IP, consulte 12.1 Función de filtro de IP en el Manual del usuario de MELSEC iQ-F FX5 (Comunicación Ethernet).

5. Referencias:

- https://www.cisa.gov/uscert/ics/advisories/icsa-22-139-01

Nombre de la alerta:

QNAP alerta a los clientes NAS de nuevos ataques de ransomware DeadBolt

Tipo de Ataque: Ransomware

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

1. Resumen:

A través del monitoreo y búsqueda de amenazas se tomó conocimiento de la publicación realizada en la página web de **BLEEPING COMPUTER**, que el fabricante de almacenamiento conectado a la red (NAS) con sede en Taiwán, QNAP, advirtió a los clientes que protejan sus dispositivos contra los ataques que impulsan las cargas útiles del Ransomware DeadBolt.

2. Antecedentes:

La compañía pidió a los usuarios que actualicen sus dispositivos NAS a la última versión de software y se aseguren de que no estén expuestos al acceso remoto a través de Internet.

Esta advertencia se produce después de otra sobre el Ransomware dirigido a dispositivos NAS expuestos a Internet publicada en enero.

3. Detalles:

QNAP aconsejó a los clientes con dispositivos de cara al público que tomaran las siguientes medidas para bloquear posibles ataques:

- Deshabilitar la función de reenvío de puertos del router: Ir a la interfaz de administración de su enrutador, verificar la configuración del Servidor virtual, NAT o Reenvío de puertos y deshabilitar la configuración de reenvío de puertos del puerto de servicio de administración de NAS (puerto 8080 y 433 de forma predeterminada).
- Deshabilitar la función UPnP del NAS de QNAP: Ir a myQNAPcloud en el menú QTS, hacer clic en "Configuración automática del enrutador" y anular la selección de "Habilitar reenvío de puertos UPnP".

Una vez implementado en un dispositivo NAS, este Ransomware utiliza AES128 para cifrar archivos, agregando una extensión .deadbolt a sus nombres.

DeadBolt también reemplaza el archivo /home/httpd/index.html para que las víctimas vean la pantalla de rescate al acceder al dispositivo comprometido.

Después de pagar el rescate, los actores de la amenaza crean una transacción de bitcoin a la misma dirección de rescate de bitcoin que contiene la clave de descifrado para la víctima (la clave de descifrado se puede encontrar en la salida de OP_RETURN).

4. **Recomendaciones:**
    - Aquellos que necesiten acceso a dispositivos NAS sin acceso directo a Internet deben habilitar la función VPN de su router (si está disponible).
    - Utilizar el servicio myQNAPcloud Link y el servidor VPN en los dispositivos QNAP proporcionados por la aplicación QVPN Service o la solución QuWAN SD-WAN.

5. **Referencias:**

- **https://www.bleepingcomputer.com/news/security/qnap-alerts-nas-customers-of-new-deadbolt-ransomware-attacks/**