Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

29-Ago-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.

Alertas de Ciberseguridad

A continuación, compartimos con ustedes algunas de las alertas más relevantes de Agosto.

Alertas de Seguridad IT:

- VirusTotal revela las principales maneras en las que el malware abusa de la confianza del usuario
- Múltiples vulnerabilidades críticas en routers Arris
- Múltiples vulnerabilidades críticas en productos Cisco
- Vulnerabilidad crítica en múltiples routers DrayTek

Alertas de Seguridad OT/ICS:

- Vulnerabilidad crítica en ConnectPort X2D Gateway de Digi International
- Vulnerabilidades críticas en bombas de infusión Baxter Sigma Spectrum

VirusTotal revela las principales maneras en las que el malware abusa de la confianza del usuario

Tipo de Ataque: Malware

Medio de Propagación: Navegación de Internet, Red, Correo

1. PRODUCTOS AFECTADOS:

- Autoridades de certificación: Sectigo (AAA), Sectigo RSA Code Signing CA, USERTrust RSA Certification y DigiCert, entre otras.
- Dominios y software legítimo.

2. RESUMEN:

Se presentaron los resultados del monitoreo y detección de VirusTotal, donde se reveló un aumento en la elaboración de ataques por medio de ingeniería social, así como diferentes métodos que buscan atacar a los sistemas vulnerables y evadir controles para instalar malware en los dispositivos de los usuarios. Distribución mediante dominios legítimos, el uso de certificaciones válidas, suplantación de aplicaciones y malware empaquetado con instaladores legítimos conforman la lista de principales amenazas sobre las cuales debemos tomar precaución.

3. DETALLE:

De acuerdo con el estudio de monitoreo y detección de amenazas de VirusTotal, se detectó un notable aumento de los ataques por medio de ingeniería social presentes en Internet. Esta creciente tendencia, junto con la distribución de software malicioso en las principales aplicaciones de comunicación, nos obligan a estar más prevenidos al momento de ingresar a páginas web o instalar programas.

Algunas de las técnicas más usadas por los atacantes para sobrepasar las defensas y hacer los ataques más efectivos son:

1. **Distribución a través de dominios legítimos**: Mediante esta modalidad los atacantes pueden evadir las defensas y alertas de los firewalls basados en dominios o IPs. Los principales dominios por donde se distribuye estos malwares son: discordapp.com, squarespace.com, amazonaws.com y mediafire.com.
2. **Certificaciones TLS válidas**: Los atacantes roban certificados legítimos y los usan para firmar su malware, de esta manera pueden ser identificados como programas desarrollados por fabricantes de software legítimos cuando no lo son. Entre las principales Autoridades de Certificación que se usan para firmar estos archivos están: Sectigo (AAA), Sectigo RSA Code Signing CA, USERTrust RSA Certification y DigiCert.
3. **Malware disfrazado de software legítimo**: Los atacantes buscan engañar a los usuarios mediante el uso de dominios e iconos similares a las principales aplicaciones usadas. Las aplicaciones más imitadas son: Skype, Adobe Acrobat, VLC y 7zip.
4. **Malware empaquetado con instaladores legítimos**: Consiste en enmascarar el malware, empaquetándolo en paquetes de instalación de software populares como: Google Chrome, Malwarebytes, Windows Update, Zoom, Brave, Firefox, etc. Este tipo de distribución puede desembocar en un ataque a la cadena de suministro, donde los atacantes logran ingresar al servidor de actualización

de un software legítimo u obtener acceso no autorizado al código fuente, lo que hace posible infiltrar el malware en forma de archivos binarios troyanos.

4. RECOMENDACIONES:

- Evitar descargar aplicaciones en tiendas de terceros.
- Actualizar el sistema operativo constantemente.
- Concientizar a los usuarios para que examinen cuidadosamente las páginas web y dominios a los que acceden.
- Desconfiar de las aplicaciones que solicitan una actualización dentro de la aplicación.

5. REFERENCIAS:

- https://blog.virustotal.com/2022/08/deception-at-scale.html
- https://thehackernews.com/2022/08/virustotal-reveals-most-impersonated.html

Múltiples vulnerabilidades críticas en routers Arris

Tipo de Ataque: Explotación de vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. PRODUCTOS AFECTADOS:

- Servidor web muhttpd, utilizado por routers que colocan los Proveedores de Servicios de Telecomunicaciones (ISP) en sus clientes, principalmente en el firmware de Arris utilizado en los modelos de router: NVG443, NVG599, NVG510, BGW210 y BGW320

2. RESUMEN:

Se reportaron múltiples vulnerabilidades críticas con relación al servidor web muhttpd, que afecta a varios modelos de routers Arris. Estas vulnerabilidades son de tipo limitación incorrecta de la ruta a un accesorio restringido, de referencia a puntero nulo y desbordamiento de búfer.

3. DETALLE:

Se detectaron múltiples vulnerabilidades existentes en el servidor web muhttpd. Este servidor web es muy utilizado en los equipos brindados por un proveedor de servicios de internet (ISP), principalmente en los modelos NVG443, NVG599, NVG510, BGW210 y BGW320 de los routers Arris. En la actualidad hay más de 19,000 routers vulnerables expuestos en Internet lo que afecta a los usuarios en general.

Entre las vulnerabilidades más críticas se encuentra la CVE-2022-31793, la cual permite a un atacante remoto, usuario sin autentificación o cualquier usuario local, recorrer las diferentes rutas de los directorios desde la raíz del sistema de archivos.

Otra vulnerabilidad que presenta es la falta de referencia de puntero NULL, debido a que el servidor muhttpd recibe múltiples solicitudes HTTP en un socket sin bloqueo. Asimismo, se presenta también un desbordamiento de búfer cuando se eliminan URL debido a que el servidor, al encontrar el símbolo “%”, intenta desencriptar los siguientes dos caracteres sin validar los límites.

4. RECOMENDACIONES:

- Identificar si se cuentan con routers Arris de los modelos mencionados y desactivar el acceso remoto hasta la actualización de los equipos.
- Para la vulnerabilidad CVE-2022-31793, Arris recomienda utilizar un firewall para evitar el acceso a redes no confiables, desactivar la gestión remota o utilizar un firewall para los puertos de acceso remoto desde internet.
- Si emplea el servidor muhttpd se recomienda actualizar a la versión 1.1.7.

5. REFERENCIAS:

- https://derekabdine.com/blog/2022-arris-advisory
- https://securityonline.info/cve-2022-31793-muhttpd-web-server-flaw-affects-arris-arris-variant-dsl-fiber-router/

Múltiples vulnerabilidades críticas en productos Cisco

Tipo de Ataque: Explotación de vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. PRODUCTOS AFECTADOS:

- Routers Cisco Small Business de la serie: RV160, RV260, RV340 y RV345.
- Cisco Webex Meetings (basado en la nube).
- Cisco Identity Service Engine (ISE): versión 2.3 y anteriores, 2.4, 2.6, 2.7, 3.0 y 3.1.
- Cisco Unified CM y Cisco Unified CM SME: versión 11.5, 12.5 y 14.
- Cisco BroadWorks Application Delivery Platform: version 22.0, 23.0 y 24.0.

2. RESUMEN:

Cisco ha informado múltiples vulnerabilidades críticas en sus productos. Estas vulnerabilidades se encontraron en distintas funciones de los dispositivos como: el portal de control web, la actualización de la base de datos del filtro web y en el Open Plug and Play. La explotación de estas vulnerabilidades podría permitir a los atacantes a causar un ataque de denegación de servicio (DoS) o inyectar comandos en el sistema.

3. DETALLE:

Se detectaron múltiples vulnerabilidades críticas en diversos productos de CISCO en el presente mes, la cuales son:

1. CVE-2022-20842 en los routers de la serie RV160, RV260, RV340 y RV345: Vulnerabilidad en el portal de control web, donde puede permitir a atacantes remotos sin autentificación realizar una ejecución arbitraria de código, o causar un reinicio del dispositivo ocasionando un ataque de denegación de servicio (DoS).
2. CVE-2022-20827 en los routers de la serie RV160, RV260, RV340 y RV345: Vulnerabilidad en la función de actualización de la base de datos del filtro web, que puede permitir a usuarios remotos no autentificados enviar información maliciosa y realizar una inyección y ejecución de comandos en el sistema operativo elemental con privilegios de root.
3. CVE-2022-20841 en los routers de la serie RV160, RV260, RV340 y RV345: Vulnerabilidad en el módulo Open Plug and Play (PnP), la cual puede permitir a atacantes remotos que puedan inyectar y ejecutar comandos en el sistema operativo subyacente. Para poder explotar esta vulnerabilidad el atacante deberá tener un punto de apoyo establecido conectado al router.

Las vulnerabilidades dependen unas de otras, por lo que los atacantes pueden aprovechar una de las vulnerabilidades para explotar otra vulnerabilidad. Asimismo, es posible que debido a las actualizaciones del software de los equipos, una vulnerabilidad no se vea afectada por el resto de vulnerabilidades.

4. RECOMENDACIONES:

- Se recomienda actualizar los productos afectados a la última versión disponible.

5. REFERENCIAS:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR
- https://nvd.nist.gov/vuln/detail/CVE-2022-20842
- https://nvd.nist.gov/vuln/detail/CVE-2022-20827
- https://nvd.nist.gov/vuln/detail/CVE-2022-20841

Vulnerabilidad crítica en múltiples routers DrayTek

Tipo de Ataque: Explotación de vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. PRODUCTOS AFECTADOS:

- Vigor3910, versiones anteriores a la 4.3.1.1
- Vigor1000B, versiones anteriores a la 4.3.1.1
- Vigor2962 Series, versiones anteriores a la 4.3.1.1
- Vigor2927 LTE Series, versiones anteriores a la 4.4.0
- Vigor2915 Series, versiones anteriores a la 4.3.3.2
- Vigor2952 / 2952P, versiones anteriores a la 3.9.7.2
- Vigor3220 Series, versiones anteriores a la 3.9.7.2
- Vigor2926 LTE Series, versiones anteriores a la 3.9.8.1
- Vigor2862 LTE Series, versiones anteriores a la 3.9.8.1
- Vigor2620 LTE Series, versiones anteriores a la 3.9.8.1
- VigorLTE 200n, versiones anteriores a la 3.9.8.1
- Vigor2133 / 2762 Series, versiones anteriores a la 3.9.6.4
- Vigor167, versiones anteriores a la 5.1.1
- Vigor130, versiones anteriores a la 3.8.5;
- VigorNIC 132, versiones anteriores a la 3.8.5
- Vigor165 / 166, versiones anteriores a la 4.2.4
- Vigor2135 / 2765 / 2766 Series, versiones anteriores a la 4.4.2
- Vigor2832, versiones anteriores a la 3.9.6
- Vigor2865 / LTE Series, versiones anteriores a la 4.4.0
- Vigor2865 / LTE Series, versiones anteriores a la 4.4.0

2. RESUMEN:

Se descubrió una vulnerabilidad crítica en múltiples routers de la marca DrayTek. La vulnerabilidad es de desbordamiento de búfer y mediante su explotación puede permitir que un atacante remoto ingrese al dispositivo, provocando una brecha en la red y obteniendo acceso no autorizado a recursos internos.

3. DETALLE:

Se detectó una vulnerabilidad crítica en los routers DrayTek. DrayTek es una compañía taiwanesa que fabrica routers de tipo SOHO (Small Office and Home Office). Cada vez más negocios pequeños o medianos implementan este tipo de routers para proporcionar un acceso más seguro a sus empleados; no obstante, hay que tener precaución y estar alertas a cubrir las vulnerabilidades que se van descubriendo.

La vulnerabilidad en los routers DrayTek, identificada como CVE-2022-32548, está presente su interfaz de gestión web. Debido a un desbordamiento de búfer en la página de login: /cgi-bin/wlogin.cgi., los atacantes pueden suministrar un nombre de usuario y/o una contraseña diseñados como cadenas

codificadas en base64 ocasionando un error lógico en la verificación del tamaño de las cadenas codificadas, lo que puede derivar en el acceso no autorizado a los recursos internos.

Esta vulnerabilidad se puede explotar mediante la red de área local (LAN) o mediante internet si es que el usuario tiene habilitada la configuración de manera remota del dispositivo. Mediante este ataque se puede obtener datos sensibles almacenados en el router (contraseñas, llaves, etc.), acceder a recursos internos localizados en la LAN que normalmente necesitarían un acceso VPN y recopilar la información que se traslada a través de algún puerto del router.

4. RECOMENDACIONES:

- Instalar el último firmware del equipo visitando la página web del fabricante
- En la página de configuración del dispositivo, verificar que las configuraciones de DNS, los accesos permitidos por la VPN u otra configuración relevante no hayan sido manipulados.

5. REFERENCIAS:

- https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/rce-in-dratyek-routers.html
- https://www.draytek.com/support/latest-firmwares/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32548

Vulnerabilidad crítica en ConnectPort X2D Gateway de Digi International

Tipo de Ataque: Explotación de vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. PRODUCTOS AFECTADOS:

- Digi ConnectPort X2D Gateway: todas las versiones de firmware en dispositivos fabricados antes de enero 2020

2. RESUMEN:

Una vulnerabilidad crítica en el producto Digi ConnectPort X2D fue reportada al CISA (Cibersecurity & Infrastructure Security Agency). Se descubrió que, en los productos fabricados antes de enero del 2020, el software realiza una operación a un nivel de privilegios superior al mínimo requerido, lo cual permite que los atacantes de manera remota puedan ejecutar un código malicioso en el sistema.

3. DETALLE:

El ConnectPort X2 es un pequeño Xbee (solución integrada que brinda un medio inalámbrico para la interconexión y comunicación entre dispositivos) que permite la ejecución de aplicaciones localmente mientras se interconecta a través de las redes Ethernet existentes para la conectividad a un servidor centralizado. Recientemente se descubrió una vulnerabilidad en los dispositivos fabricados antes de enero del 2020, la cual detalla que el dispositivo tenía privilegios innecesarios para su funcionamiento.

La vulnerabilidad CVE-2022-2634 es una vulnerabilidad hallada en el dispositivo Digi ConnectPort X2D, la cual permite a los atacantes escalar en los privilegios del sistema de manera remota. Esta vulnerabilidad existe debido a la falta de protecciones en los accesos y permisos cuando se usa la aplicación web.

Atacando la vulnerabilidad se pueden subir arbitrariamente archivos codificados en Python y ejecutar el código en el sistema con los permisos adquiridos. Debido a esto, la vulnerabilidad detectada fue catalogada como crítica.

4. RECOMENDACIONES:

- Identificar los controladores vulnerables y actualizarlos con la última versión de firmware disponible.

5. REFERENCIAS:

- https://www.cisa.gov/uscert/ics/advisories/icsa-22-216-01
- https://www.cybersecurity-help.cz/vdb/SB2022080514
- https://www.digi.com/xbee
- https://nvd.nist.gov/vuln/detail/CVE-2022-2634

Vulnerabilidades críticas en bombas de infusión Baxter Sigma Spectrum

Tipo de Ataque: Explotación de vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. **PRODUCTOS AFECTADOS:**

- Sigma Spectrum v6.x modelo 35700BAX
- Baxter Spectrum v8.x modelo 35700BAX2
- Baxter Spectrum v9.x modelo 35700BAX3
- Sigma Spectrum LVP v6.x con Wireless Battery módulos v9, v11, v13, v14, v15, v16, v16D38, v17, v17D19, v20D29 hasta v20D32, y v22D24 hasta v22D28
- Baxter Spectrum LVP v8.x con Wireless Battery módulos v17, v17D19, v20D29 hasta v20D32, and v22D24 hasta v22D28
- Baxter Spectrum LVP v9.x con Wireless Battery módulos v22D19 hasta v22D28

2. **RESUMEN:**

El equipo de CISA publicó las principales vulnerabilidades que afectan a las bombas de infusión Baxter Sigma Spectrum. Se revelaron fallos en la configuración y distintas vulnerabilidades críticas de las que los atacantes podrían aprovecharse para acceder a información sensible o manejar de manera remota los distintos dispositivos.

3. **DETALLE:**

Se descubrieron vulnerabilidades críticas en las bombas de infusión Baxter Sigma Spectrum utilizados en la industria médica para ayudar a prevenir errores médicos y mejorar la seguridad del paciente. Al explotar estas vulnerabilidades el atacante podría acceder a información sensible, y alterar la configuración del sistema, así como la disponibilidad del mismo.

Dentro de un listado de 6 vulnerabilidades, las principales a resaltar son:

1. Envío de información sensible sin codificar: En la capa de aplicación de algunos de los dispositivos afectados, se utiliza un canal de comunicación sin cifrado ni autentificación para enviar y recibir información operativa. Esto puede permitir que un atacante que haya eludido las medidas de seguridad de la red pueda ver información confidencial o realice un ataque Man-in-the-Middle.
2. Manejo remoto y manipulación: Algunos dispositivos operan con un protocolo Telnet con credenciales incrustadas en el código (hard-coded credentials) cuando se conectan a SSIDs específicos. Esta manipulación permite acceso a información sensible, cambiar la configuración de red o reiniciar el dispositivo.
3. Uso de un recurso después de su expiración: Al configurar la red inalámbrica de algunos dispositivos, se le permite al FTP continuar operando hasta que el dispositivo se reinicie.

4. RECOMENDACIONES:

- Baxter recomienda usar los protocolos de seguridad de red inalámbrica más seguros (WPA2, EAP-TLS, etc) para que haya una autentificación y encriptación de la información mandada hacia y desde un dispositivo.
- Se recomienda minimizar la exposición de los dispositivos/sistemas de control y asegurar que no sean accesibles desde internet.
- Cuando se requiera acceso remoto, utilizar métodos seguros como VPNs.

5. REFERENCIAS:

- https://www.cisa.gov/uscert/ics/advisories/icsma-20-170-04
- https://cwe.mitre.org/data/definitions/672.html
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-12040
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-12047
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-12043