Boletín de Ciberseguridad

Fecha de Publicación
16/08/2021 - N.º 14

Mes de Agosto
02/08/2021 - 16/08/2021

Datasec

Índice

Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención. La publicación de dichas noticias dependerá de la importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta segunda quincena del mes de agosto se destacan 6 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, 1 de fraude activos y 3 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Son publicadas fallas de consideración para productos Cisco

Recientemente han sido identificadas varias fallas de consideración critica en productos CISCO, lo que podría permitir a un atacante remoto no autenticado ejecutar código arbitrario o causar una condición de denegación de servicio (DoS) a través del envío de peticiones HTTP.

Routers comprometidos por fallo de seguridad

Especialistas alertan sobre routers que han sido comprometidos por un fallo de seguridad que evita la autenticación y afecta a dispositivos que utilizan el firmware Arcadyan. En el caso de que se dé una explotación exitosa, el atacante podría acceder y tomar el control, realizando ataques mediante la botnet Mirai.

Microsoft IIS Servers es afectado por una APT Hacking

Se advierte sobre un ataque persistente en EE.UU. que está siendo dirigido hacia los principales organismos públicos y privados del país. El mismo consiste en la intrusión de servidores de Microsoft Internet Information Services (IIS), mediante una nueva APT Hacking con el seudónimo de Mantis religiosa o TG2021.

La amenaza del Ransomware en la actualidad

Es incontable la cantidad de ataques de fuerza bruta diarios observados mediante la utilización de ransomware, un tipo de programa que explota las fallas de seguridad informáticas de una empresa o individuo, paralizando sus sistemas para exigir una recompensa a cambio del desbloqueo.

CISCO	**Son publicadas fallas de consideración para productos Cisco**	CRÍTICO

Descripción

Recientemente han sido identificadas varias fallas de consideración critica en productos CISCO, lo que podría permitir a un atacante remoto no autenticado ejecutar código arbitrario o causar una condición de denegación de servicio (DoS) a través del envío de peticiones HTTP.

La principal preocupación radica en una de estas fallas, que refiere a una incorrecta validación de las peticiones HTTP en la interfaz web de administración de los enrutadores Dual WAN Gigabit VPN, la cual se determinó con una valoración CVSS de 9.8 sobre 10.

Afectados

- Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers Web Management.
- Cisco Small Business RV160 and RV260 Series VPN Routers.
- Cisco Packet Tracer for Windows DLL Injection.
- Cisco Network Services Orchestrator CLI Secure Shell Server.
- ConfD CLI Secure Shell Server.

Estado

"Dicha interfaz de administración web es accesible localmente de manera predeterminada y no se puede deshabilitar. Por otra parte, aunque el acceso remoto debe ser configurado por el usuario y se encuentra desactivada por defecto, se ha podido comprobar la existencia de más de 8.800 dispositivos accesibles de forma remota."

Otro de los problemas graves también es debido a un fallo en la interfaz web de administración y su explotación es similar a la anterior, aunque en este caso sí se requiere de autenticación.

De los ataques detectados, se observan:

- Ejecución de código remoto.
- Escalada de privilegios.
- Ataque de inyección de DLL por parte de un atacante local sin autenticar.
- Ejecutar comandos arbitrarios con los permisos de la cuenta bajo la cual se ejecuta Cisco NSO o ConfD (root de forma predeterminada). Debido a una incorrecta ejecución del servicio de usuario SFTP con el nivel de privilegio de la cuenta que se estaba utilizando cuando se habilitó el servidor Secure Shell (SSH) integrado.

Remediación / Referencias

En el sitio oficial de Cisco se puede encontrar las actualizaciones correspondientes para la correcta mitigación de estas fallas.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2021/08/graves-vulnerabilidades-en-productos.html
https://unaaldia.hispasec.com/2021/08/graves-vulnerabilidades-en-productos-cisco.html

	**Routers comprometidos por fallo de seguridad**	CRÍTICO

Descripción

Especialistas alertan sobre routers que han sido comprometidos por un fallo de seguridad que evita la autenticación y afecta a dispositivos que utilizan el firmware Arcadyan. En el caso de que se dé una explotación exitosa, el atacante podría acceder y tomar el control, realizando ataques mediante la botnet Mirai.

Se trata de un malware de la familia de las botnets que busca infectar dispositivos de tipo IoT. El objetivo de esta botnet es la infección de routers y cámaras IP para realizar ataques de tipo DDoS
Esta vulnerabilidad ha sido calificada con una valoración CVSS de 9,9 puntos sobre 10 por su criticidad.

Afectados

Se estima que puede haber millones de routers afectados en todo el mundo, perjudicando una gran cantidad de modelos y operadoras de telefonía como, British Telecom, Deutsche Telecom, Orange, O2 (Telefónica) o Vodafone. Repercute tanto a modelos de ADSL como de fibra.

Invitamos a acceder al siguiente link para ver los modelos y proveedores afectados.

- https://es-la.tenable.com/security/research/tra-2021-13

Este error de seguridad no solo afecta a routers, sino que también deja expuestos dispositivos IoT que cuentan con el mismo código base vulnerable.

Estado

Esta vulnerabilidad ha estado presente durante una década y luego de que se publicara una prueba de concepto, hace unas pocas semanas, ya se han empezado a detectar ataques.

Investigadores en ciberseguridad explican que el problema radica en que, una gran cantidad de los usuarios de este tipo de router, no han realizado las actualizaciones correspondientes de los modelos utilizados y pueden quedar expuestos a un ataque mediante este tipo de malware.

Remediación / Referencias

Recomendamos actualizar el firmware del router utilizado por el usuario y de los dispositivos que estén conectados a Internet.

Por mayor información invitamos a visitar los siguientes sitios:
https://blog.segu-info.com.ar/2021/08/vulnerabilidad-grave-en-millones-de.html
https://www.bleepingcomputer.com/news/security/actively-exploited-bug-bypasses-authentication-on-millions-of-routers/

DHL	**Malware activo e intento de Phishing con sitio web fraudulento**	IMPORTANTE

Descripción

Fuentes oficiales han identificado la presencia de un malware activo, que mediante un sitio fraudulento intenta suplantar a DHL Express. Los ciberdelincuentes intentan persuadir a los usuarios mediante el envío de un correo electrónico que contiene un archivo adjunto para descargar y ser ejecutado infectando el dispositivo del usuario.

Este intento de Phishing consiste en que la víctima descargue este malware, siendo engañado por el asunto del correo, el cual que indica que el archivo es un documento de embarque.

Afectados

DHL es la empresa de envió de correspondencia más importante a nivel mundial, integrada desde 2002 en el grupo Deutsche Post DHL, con sede principal en Alemania.

Para el 2020 DHL contaba con 380.000 funcionarios y realizó 484 millones de envíos en total para sus clientes (B2C y B2B), en todo el mundo, un 9% más por día que en 2019.

Estado

Solicitamos tener en consideración las señales de compromiso en su conjunto:

Datos del encabezado del correo
Servidores SMTP
208.76.251[.]250

Correo Electrónico: postmaster@loft-dev.live

Archivos que se encuentran en la amenaza

Nombre: DHL Documentos De Envío Originales.zip

SHA256: AE680810C7CE9D5415715CB2960828EB9BC4B3AD9494138CC1892B852E0B5112

Nombre: xVJqtDSapgmxlOP.exe

SHA256: 42B4A1C6BB6C57B21540D10A07B8E94F282C75909D218734A6872137857A2E8F

Remediación / Referencias

Recomendaciones:

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

Por mayor información invitamos a visitar los siguientes sitios:
https://www.csirt.gob.cl/alertas/2cmv21-00210-01/

Medidas para resguardar información sensible en dispositivos IoT

PREVENCIÓN

Descripción

"El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México (INAI) alertó del riesgo a la privacidad que provoca el uso de aparatos electrónicos que utilizan la tecnología denominada Internet de las Cosas (IoT, por sus siglas en inglés) dado que utilizan datos personales."

Afectados

El Internet de las cosas (IoT) es el proceso que permite conectar elementos físicos cotidianos a Internet: desde objetos domésticos comunes, hasta recursos para la atención de la salud, como los dispositivos médicos; también incluyen prendas y artículos personales, como los relojes inteligentes, e incluso los semáforos en ciudades inteligentes.

Vector de Ataque

Hasta ahora, subrayó, no se encuentran definidos los requisitos mínimos de seguridad que deben cumplir los fabricantes de equipos IoT, por ello, la información que almacenen puede ser utilizada para generar patrones de conducta o consumo, pero también puede ser captada por ciberdelincuentes.

Es importante destacar que este tipo de dispositivos inteligentes pueden detectar, almacenar, procesar o transmitir información personal, a través de una interconexión de internet, como el estado de salud, datos biométricos, hábitos y consumos, entre otros. Es debido a esto que, si no se toman las medidas de precaución necesarias, la información de los usuarios puede quedar expuesta a ser vulnerada.

Remediación / Referencias

Se recomienda a los usuarios de dispositivos con tecnología IoT, las siguientes medidas preventivas:

- Verificar el tipo y cantidad de datos que obtienen los dispositivos inteligentes.
- Modificar la configuración en función de las necesidades del usuario, conservando siempre las medidas de seguridad instaladas por defecto.
- Revisar quién o quiénes tienen acceso a la información recabada o si existe la posibilidad de un acceso remoto a ellos, configurando los parámetros de seguridad convenientes.
- Leer las condiciones de uso y almacenamiento de la información, considerando que pueden recoger datos, procesarlos y compartirlos.
- Informarse antes de comprar un dispositivo y adquirir los que resulten más seguros, por ejemplo: aquellos que permitan actualizaciones de seguridad, y faciliten el borrado de datos personales cuando sean desechados o transferidos a otro propietario.
- Cambiar las contraseñas de fábrica y establecer unas seguras, que contengan más de 8 caracteres en letras minúsculas y mayúsculas, dígitos y caracteres especiales.
- Habilitar el acceso a internet solo cuando sea necesario y en redes que sean seguras.
- Instalar aplicaciones desde los canales oficiales facilitados por los fabricantes.
- Mantener actualizado el software del dispositivo, para contar con los parches más recientes, provistos por el fabricante y asegurar que sean remediadas las vulnerabilidades conocidas.
- Evitar vincular el dispositivo inteligente a otros aparatos de los que se desconoce su nivel de seguridad.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/08/riesgos-la-privacidad-en-dispositivos.html
https://www.redhat.com/es/topics/internet-of-things/what-is-iot

Microsoft IIS	Microsoft IIS Servers es afectado por una APT Hacking	PREVENCIÓN

Descripción

Se advierte sobre un ataque persistente en EE.UU., que está siendo dirigido hacia los principales organismos públicos y privados del país. El mismo consiste en la intrusión de servidores de Microsoft Internet Information Services (IIS), mediante una nueva APT Hacking con el seudónimo de Mantis religiosa o TG2021.

Afectados

- Servidores de Microsoft Internet Information Services (IIS).
- Ataques dirigidos a organizaciones comerciales.

Vector de Ataque

APT: Se trata de un ataque que persiste en el tiempo, y es llevado a cabo por un conjunto de procesos informáticos creados con la intención de seleccionar un objetivo determinado de una manera silenciosa, vulnerando el dispositivo de la víctima, para en este caso elevar privilegios.

Las vulnerabilidades detectadas son:

- Exploit RCE de encuesta de casilla de verificación.
- Explotación de deserialización VIEWSTATE.
- Altserialización insegura.
- Exploit de Telerik-UI.

“Esta nueva APT utiliza un framework de malware personalizado, construido alrededor de un núcleo común, hecho a la medida para los servidores IIS. El conjunto de herramientas es completamente volátil, se carga de manera reflectante en la memoria de una máquina afectada y deja poco o ningún rastro en los objetivos infectados", el dijeron los investigadores. El actor de amenazas también utiliza una puerta trasera sigilosa adicional y varios módulos posteriores a la explotación para realizar el reconocimiento de la red, elevar los privilegios y moverse lateralmente dentro de las redes.”

Para la llevar adelante este tipo de ataque, los ciberdelincuentes también se aprovechan de la explotación de aplicaciones web ASP.NET, creando una puerta trasera de los servidores mediante la ejecución de un implante sofisticado llamado "NodeIISWeb". El mismo fue creado con el fin de interceptar y controlar las solicitudes HTTP que recibe el servidor, además de cargar archivos DLL específicos.

Remediación / Referencias

Se recomienda estar continuamente informado del avance de este tipo de amenazas.

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/08/nueva-apt-hacking-apunta-microsoft-iis.html
https://thehackernews.com/2021/08/new-apt-hacking-group-targets-microsoft.html

	La amenaza del Ransomware en la actualidad	PREVENCIÓN

Descripción

Es incontable la cantidad de ataques de fuerza bruta diarios observados, mediante la utilización de ransomware, un tipo de programa que explota las fallas de seguridad informáticas de una empresa o individuo, paralizando sus sistemas para exigir una recompensa a cambio del desbloqueo.

El ransomware se ha convertido en el vector de ataque por excelencia elegido por grupos de cibercriminales para recaudar dinero mediante técnicas extorsivas. Esto es debido a que la distribución de este tipo de ataques no era de consideración en el pasado y una gran cantidad de empresas no tomaron las medidas de precaución necesarias, descuidando así su seguridad.

“Entre enero de 2020 y junio de 2021, la protección contra ataques de fuerza bruta de ESET evitó más de 71 mil millones de ataques contra sistemas con el puerto al Protocolo de escritorio remoto (RDP) accesible de manera pública, lo que demuestra la popularidad de ese protocolo entre los ciberdelincuentes como superficie de ataque. Si bien el crecimiento más notable se produjo en la primera mitad de 2020, cuando se decretaron en el mundo las primeras cuarentenas debido a la pandemia, los picos diarios más altos se registraron en la primera mitad de 2021.”

Afectados

Por el momento es difícil estimar el alcance real del ataque con "ransomware",

Recientemente se pudo confirmar muchos ataques a cadena de suministros y se han vuelto frecuentes en varios países, afectando la operativa normal de organizaciones sin discriminar rubro. Algunos ejemplos son los casos de la empresa frigorífica JBS y el operador de oleoductos Colonial Pipeline, así como a comunidades y hospitales, entre otros.

Se han pagado sumas de hasta $70 millones de dólares, a grupos delictivos como REvil en el ataque de Kaseya y $40 millones pagados por la compañía de seguros CNA, lo que demuestra el avance de esta amenaza en la actualidad.

"La comparación del primer semestre de 2020 con el primer semestre de 2021 muestra un enorme crecimiento del 612% de estos ataques que buscan adivinar las contraseñas y que apuntan al RDP (Remote Desktop Protocol). El número promedio diario de clientes únicos que reportan este tipo de ataques también ha aumentado significativamente, pasando de 80.000 en el primer semestre de 2020 a más de 160.000 (más del 100%) en el primer semestre de 2021."

Vector de Ataque

Son muchas las estrategias utilizadas para vulnerar a las víctimas, pero se destaca la extorsión (o doxing), una técnica que fue detectada por primera vez en el año 2019 siendo implementada por ransomware Maze, el cual parece haber cesado sus actividades.

Otras de ellas, es adquirir vulnerabilidades zero-day y comprar credenciales robadas en la Deep web.

El ataque sobre el RDP (Remote Desktop Protocol) también es una de las técnicas más utilizadas en la actualidad. A esto le siguen, la distribución de archivos fraudulentos, macros maliciosas, hipervínculos dañinos y binarios de botnets, además de una gran cantidad de ataques de fuerza bruta.

A continuación, algunas de las Familias de Ransomware identificados más importantes:

- Sodinokibi (también conocido como REvil).
- Avaddon.
- DoppelPaymer.
- Ryuk.
- Maze.

Remediación / Referencias

Recomendamos tener especial atención antes los múltiples incidentes reportados por los sitios de confianza y seguir informándose en los avances de las nuevas técnicas de prevención Antimalware.

"La implementación de políticas, la adecuada configuración del acceso remoto, y el uso de contraseñas seguras en combinación con la autenticación multifactor, pueden ser los elementos decisivos en la lucha contra el ransomware. La importancia de instalar las actualizaciones de seguridad a tiempo, ya que las vulnerabilidades divulgadas y reparadas (pero sin parchear) se encuentran entre los vectores de interés de estas bandas."

Por mayor información al respecto se puede acceder a:
https://www.welivesecurity.com/la-es/2021/08/10/ransomware-no-detiene-como-combatir-amenaza/

Conclusiones

Se están haciendo cada vez más presentes los ataques de extorsión a todo nivel, tanto a personas como empresas y los medios tecnológicos que estos utilizan, de esta manera surgen aseguradoras para elevar el nivel de confianza y prevenir o ayudar en la recuperación.

En ese sentido, es importante por parte de las aseguradoras evitar los riesgos lo máximo posible, es así que a varios niveles los planes de capacitación, concientización y hábitos de mejores prácticas seguras de la información se están haciendo cada vez más omnipresentes.

Esto permitirá que todas las personas involucradas en los diferentes procesos de manejo de información, conozcan los medios para identificar y manejar de forma segura y garantizar así que la misma se limite a sus cometidos, y así nuestras acciones de gestión de software, hardware y equipos de trabajo sea primero mediante las metodologías ajustadas a los niveles de seguridad esperados sobre tales elementos de información.

Tanto en estos procesos como en los cada vez más frecuentes "takedown," a los que se enfrentan sobre todo las organizaciones modernas para enfrentar desafíos de falsificación, fuga de información y de amenazas persistentes, sobre internet, se ve cada día más la participación e interrelación entre técnicos y otros actores como abogados y especialistas en leyes, que confluyen para garantizar los mecanismos de protección necesarios.

Nuestro trabajo sigue siendo encaminar y facilitar la adopción de mecanismos de protección, de forma tal que las organizaciones mantengan procesos seguros de forma consciente e integrados en el quehacer diario. Desde Datasec seguimos apoyando desde las áreas de capacitación, como técnicas y de auditoría a los diferentes actores para aunar así los esfuerzos y reducir la complejidad que representa el mundo de la ciberseguridad.

¡Sigamos cuidándonos!