SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]

AÑO 02 EDICIÓN 2.31

WWW.COREONEIT.COM
@COREONEIT

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

¿QUÉ ES EL SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]?

Es una combinación de información de amenazas existentes en la red con el análisis e inteligencia del grupo de especialistas de CORE ONE IT, quienes analizan exhaustivamente todo tipo de amenazas informáticas y desarrollan una serie de recomendaciones adaptadas a cada tipo de cliente.

ALCANCE

Se personaliza de acuerdo al tipo de infraestructura y entorno de red del cliente basado en los tipos de dispositivos, modelos y fabricantes, con el fin de recibir solo información relevante y que pudiera afectar de manera directa o indirecta, la continuidad del negocio.

DEFINICIONES

•Riesgo: Probabilidad que una amenaza particular explote una vulnerabilidad particular de un sistema.

•Amenaza: Es la causa potencial de un incidente no deseado, el cual puede resultar en un daño a un sistema de información u organización.

•Ataque: Acción de tratar de traspasar controles de seguridad en un sistema. Un ataque puede ser activo, resultando en la modificación de datos, o pasivo, resultando en la divulgación de información. El hecho de que un ataque sea realizado no significa que será exitoso, el grado de éxito depende de la vulnerabilidad del sistema o actividad y de la eficiencia de las medidas existentes.

•Vulnerabilidad: Debilidad en los procedimientos de seguridad de un sistema, en el diseño del sistema, en la implementación, en los controles internos, y que puede ser explotada para violar la política de seguridad del sistema.

•API: Interfaz de Programación de Aplicaciones (Application Programming Interface, por sus siglas en inglés). Conjunto de subrutinas, funciones y procedimientos de una biblioteca para ser utilizado por otro software

•Malware: también llamado badware, código maligno, software malicioso, software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

•Ransomware: Es un tipo especial de malware que amenaza con destruir los documentos y otros archivos de las víctimas.

•Troyano: Software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo.

•ISP: Proveedor de servicios de Internet (Internet Service Provider, por sus siglas en inglés)

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

MINIMICE EL IMPACTO DEL RANSOMWARE CON LA PREVENCIÓN, CONTINUIDAD Y RECUPERACIÓN BASADAS EN LA NUBE.

El Ransomware plantea una amenaza grande y creciente a las organizaciones de todos los tamaños, desde empresas grandes a pequeñas y agencias del gobierno. ¿Qué es ransomware? Es un tipo de esquema de Cyber-extorsión que involucra un malware que cifra los datos y los archivos en las PC's de las víctimas, servidores u otros sistemas, lo que los hace inutilizables. Una vez desplegado, el atacante exige el pago de un rescate a cambio de una clave de descifrado, que desbloquea los archivos para que puedan ser nuevamente utilizados.

El Informe de Investigaciones de Violación de Datos de 2017, décima edición, las soluciones empresariales de Verizon encontraron que los incidentes de Ransomware subieron del puesto número 22 de ataques más comunes de malware en el 2014 a la posición número 5 en el 2017, el informe también encontró que el correo electrónico se posiciono como el principal vector de malware en el 2017. Los costos globales del daño causado por un Ransomware se estima que exceden los $5 mil millones en 2017, en comparación con los $325 millones en 2015.

Los enfoques actuales se quedan cortos

Muchas organizaciones equivocadamente creen que su antivirus y otros productos de seguridad orientados a la prevención los protege lo suficiente contra el ransomware. También suelen pasar por alto los escenarios de Ransomware al formular sus planes de continuidad o de recuperación ante desastres. Sin embargo, según la firma de analistas de TI Gartner, Inc., los atacantes que hacen uso del Ransomware cambian constantemente sus tácticas y el propio código del malware para evadir las defensas de los antivirus.

La rápida evolución de la naturaleza de este tipo de delitos hace que la gestión del riesgo del Ransomware se vuelva una cuestión de qué hacer cuando, en lugar de si su organización es atacada.

La necesidad de una estrategia multifacética

Frente a la constante escalada de las amenazas de Ransomware, así como el dolor y el costo de restaurar las operaciones después de un ataque, una estrategia efectiva para administrar el riesgo del Ransomware transmitido por correo electrónico necesita ser multifacética, e incluir medidas para:

- *Prevenir que el Ransomware llegue a la organización.*
- *Mantener la continuidad del correo electrónico en caso de que el Ransomware haya entrado, y*
- *Recupere los servicios de correo electrónico y los datos de forma rápida y con una interrupción mínima en las operaciones del negocio.*

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Conclusión

A medida que los ataques de ransomware continúan proliferando, las organizaciones se enfrentarán a una creciente presión para proteger los recursos digitales sensibles. Sin embargo, ni los enfoques preventivos ni remediadores ofrecen una protección completa. Las organizaciones pueden fácilmente implementar y administrar una defensa en capas en contra del Ransomware.

FUENTES:

Minimice Ransomware's Impact. (2017). 1a ed. [ebook] infosecurity group. Disponible en: https://www.infosecurity-magazine.com/white-papers/minimize-ransomwares-impact/ [Consultado 4 Nov. 2017].

UNA DETECCIÓN OPORTUNA DE UN ATAQUE REDUCE EL COSTO DE RECUPERACIÓN A LA MITAD Y LOS GERENTES NO LO SABEN

Muchas empresas en Europa han descubierto que han sido atacados casi al instante y asumen sus costos bajo una media de recuperación de 456.000 dólares frente al más de 1 millón de dólares que tendrían que afrontar si se tardarán más de una semana.

Por un lado nunca debemos dejar de lado la prevención en materia de ciberseguridad, Kaspersky Lab advirtió del peligro que significa no estar preparados para el riesgo. Las empresas deberían saber cómo detectar ataques y responder en consecuencia (Estar preparados) ¿Usted lo está?

Según datos que maneja la compañía Kaspersky, sólo 1 de cada 4 empresas fue capaz de descubrir en un día el incidente de seguridad más grave durante el último año 2017.

Lo que quizás no saben los directivos y gerentes de cada una de las empresas que tardaron en descubrir los incidentes de seguridad más de una semana es que esto trae consecuencias financieras que impactan de muy diferentes maneras a la organización que intentan llevar adelante. Lidiar con el coste de 1,2 millones de dólares que deben enfrentar las organizaciones que tardan más de una semana en descubrir una amenaza, aquellas que lo hacen de inmediato reducen el coste medio de recuperación por más de dos, hasta los 456.000 dólares.

El informe de Kaspersky Lab dice: New Threats, New Mindset: Being Risk Ready in a World of Complex Attacks (Es decir: Nuevas amenazas, nueva mentalidad: estar preparado para el riesgo en un mundo de ataques complejos) el informe reveló que los ataques dirigidos están aumentado en frecuencia y en complejidad y la cuota que no es muy alentadora es que el 52 % de las compañías les resulta difícil distinguir entre ataques genéricos y ataques complejos. El número de organizaciones que asumen el hecho de que acabarán sufriendo una brecha de seguridad aumenta, mientras el 42 % no está seguro de cuál es la estrategia de respuesta más efectiva (es el caso de latino américa). Y eso que un 77 % creen que están gastando lo suficiente, o incluso demasiado, en temas de protección para ataques dirigidos.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

"Esto tal vez se deba a cómo se percibe la protección contra amenazas", razonan desde Kaspersky Lab, que explica que "a veces las amenazas simplemente se ven como un problema técnico que se resuelve comprando e implementando soluciones de ciberseguridad más avanzadas. Sin embargo, un enfoque más equilibrado en la respuesta a incidentes incluye invertir no solamente en las tecnologías correcta, sino también en personas con habilidades específicas, y en los procesos adecuados".

Desde Kaspersky recomiendan aumentar contar personal ligado a áreas de seguridad defensiva, seguridad ofensiva, para en conjunto realizar manejos de incidentes, la relevancia de la respuesta ante incidentes dentro de las responsabilidades que se atribuyen a los departamentos de seguridad TI. "Para las organizaciones, esto no significa estar exento de riesgos", indica Alessio Aceti, responsable de la Enterprise Business Division de Kaspersky Lab, "ayudará a prepararse para el riesgo y a sobrevivir a una violación grave cuando suceda".

FUENTES:

enHacke. (2017). Una detección oportuna de un ataque reduce el costo de recuperación a la mitad y los gerentes no lo saben. Noviembre 2017, de enHacke Sitio web: http://www.enhacke.com/2017/11/03/deteccion-oportuna-de-un-ataque/

IOT_REAPER, LA NUEVA BOTNET IOT QUE ESTÁ SUPERANDO A MIRAI

Hace aproximadamente un año, la botnet Mirai lanzaba un ataque DDoS que dejó sin servicio a medio Internet. Esta botnet, que había pasado desapercibida durante meses, había consiguió tomar el control de millones de dispositivos del Internet de las cosas, posicionándose como una red zombie de lo más peligrosa. A pesar de que esta botnet no ha dejado de crecer, otras han intentado robarle protagonismo lanzando nuevos ataques informáticos y, justo un año después de sus primeros ataques, parece que una nueva botnet está a la altura de Mirai, y cerca de superarla: IoT_reaper.

IoT_reaper es una nueva red zombie formada, principalmente, por todo tipo de dispositivos del Internet de las cosas. Esta red ha estado creciendo en silencio sin levantar las sospechas de los investigadores de seguridad hasta que fue detectada por primera vez el pasado mes de septiembre. Desde entonces, empresas como Qihoo 360 han empezado a estudiar su funcionamiento y han descubierto que se trata de una red zombie que está creciendo exponencialmente y que en muy poco puede llegar a superar a Mirai, poniendo de nuevo en jaque a todo Internet.

A diferencia de otras botnets, esta no trata de romper contraseñas con diccionario o fuerza bruta, sino que directamente utiliza exploits con los que aprovecharse de un gran número de vulnerabilidades en todo tipo de dispositivos IoT, especialmente de los siguientes fabricantes:

- *Dlink (routers)*
- *Netgear (routers)*
- *Linksys (routers)*
- *Goahead (cámaras IP)*
- *JAWS (cámaras IP)*
- *AVTECH (cámaras IP)*
- *Vacron (NVR)*

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

En estos momentos, los expertos de seguridad calculan que esta botnet tiene un total de dos millones de dispositivos, pero su preocupante crecimiento le hace ganar más de 10.000 nuevos "zombies" al día.

Si tenemos en cuenta que Mirai logró tumbar DynDNS con "solo" 100.000 dispositivos IoT, esta nueva botnet puede llegar a ser mucho más peligrosa de lo que cabría esperar.

Cómo proteger nuestros dispositivos para que no pasen a formar parte de IoT_Reaper

Como hemos dicho, esta botnet no "rompe" las contraseñas de los dispositivos, por lo que, aunque utilicemos una contraseña segura en ellos, no estarán correctamente protegidos.

Al ser un ataque basado en exploits que se aprovechan de vulnerabilidades, la única solución es instalar las últimas versiones de los firmwares de todos estos dispositivos con el fin de que, con suerte, solucionen estas vulnerabilidades e impidan que el exploit se ejecute. En el caso de que nuestros dispositivos estén dentro de una red de empresa, también es posible utilizar técnicas de mitigación avanzadas que analicen la red y bloqueen estos exploits.

Mientras esta botnet sigue creciendo, los expertos de seguridad advierten de otra amenaza similar, llamada IoTroop, que está tomando el control de cientos de cámaras IP de una gran variedad de fabricantes, como GoAhead, D-Link, TP-Link, AVTECH, Linksys y Synology, entre otros.

Es muy posible que pronto veamos cómo alguna botnet vuelve a poner en peligro a Internet, como ha hecho Mirai y como han hecho otras botnets. Y es que, a pesar de los estragos que causan los ataques DDoS, aún no hay ninguna forma realmente eficaz de protegernos de ellos. Y menos cuando su ancho de banda supera las varias decenas de gigabits por segundo.

FUENTES:

blog.netlab.360.com (2017). IoT_reaper: A Rappid Spreading New IoT Botnet. http://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/

Traducción recuperada de:

SoftZone (2017). IoT_reaper, la nueva botnet IoT que está superando a Mirai. noviembre 01, 2017. https://www.softzone.es/2017/11/01/iot-reaper-botnet/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

PARCHE DE SEGURIDAD PARA WORDPRESS MITIGARÍA INYECCIÓN SQL

Con su versión más reciente, WordPress incluyó un parche de seguridad que mejoró enormemente la resistencia de la plataforma a inyecciones SQL, lo cual puede permitir a atacantes el control de un sitio.

El lanzamiento de la versión 4.8.3 sucede a la actualización anterior que falló en la mitigación de la misma falla y causó problemas adicionales a algunos desarrolladores, según reportó Anthony Ferrara, investigador de seguridad y vicepresidente de ingeniería en Lingo Live. Ferrara resaltó que mientras los fixes anteriores apaciguaron ciertos comportamientos que pudieran haber sido explotados, aún contenía vulnerabilidades que permitían a plugins maliciosos y desarrolladores de temas el llevar a cabo inyección SQL.

Mitigando la amenaza de la inyección SQL

La preocupación de Ferrara se centraba en el uso de funciones preparadas utilizadas en consultas. Los marcadores de posición en un código de consulta pueden ser burlados para representar caracteres que cambien el flujo destinado del programa. Básicamente, el fix 4.8.2 puso un filtro en frente de las funciones de consulta para eliminar todos los caracteres no aprobados, lo cual fuerza la detención del comportamiento específico mostrado en la vulnerabilidad original.

Aun así, Ferrara cree que el verdadero problema fue que WordPress ha pasado las entradas de usuario al lado de consultas de la función de preparación, aun cuando haya pasado a través de una función de escape, como el filtro del 4.8.2. Por lo tanto, la función de "doble preparación" fue fundamentalmente problemática, debido a que podría llevar a un valor no confiable que fuese colocado en una consulta final.

Conflicto de Intereses

De acuerdo con SecurityWeek, Ferrara imploró a los desarrolladores de plugin y proveedores de hosting que parcharan sus productos contra la falla. Esto probablemente incitó a WordPress, el cual había sido reticente a lanzar un parche precipitadamente debido a las preocupaciones de que pudiera desatar fallas en ciertas funciones, a priorizar la vulnerabilidad y lanzar una solución más completa con la versión 4.8.3. La nueva actualización incluye una revisión adicional para preparaciones dobles. Este escenario ilustra las prioridades conflictivas de quienes desarrollan productos y quienes deben apoyarlos. Los desarrolladores pueden ser reacios a realizar diseños adicionales únicamente para compensar fallas de seguridad, pero los proveedores no pueden exponer a sus usuarios a vulnerabilidades conocidas. Es por eso que es fundamental encontrar el equilibrio correcto entre la seguridad y la experiencia del usuario.

FUENTES:

Larry Loeb (2017). WordPress Issues Security Patch to Mitigate SQL Injection, de Security Intelligence. Sitio web: https://securityintelligence.com/news/wordpress-issues-security-patch-to-mitigate-sql-injection/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDADES CRÍTICAS DE SEGURIDAD PARA TOMAR LAS MEDIDAS PREVENTIVAS Y CORRECTIVAS FRENTE A LAS AMENAZAS TECNOLÓGICAS

JUNOS: VULNERABILIDAD POTENCIAL DE EJECUCIÓN REMOTA DE CÓDIGO EN PAM (CVE-2017-10615)

Criticidad: Alta
Impacto: Ejecución de código
Vulnerabilidad:
Ejecución: Remota
Plataforma(s)
afectada(s): Junos OS 14.1, 14.1X53, 14.2.
Referencia: CCVE-2017-10615

Descripción:

Una vulnerabilidad en el módulo de autenticación conectable (PAM) de Juniper Networks Junos OS puede permitir que un atacante basado en red no autenticado ejecute código arbitrario o daemons bloqueados como telnetd o sshd que hacen uso de PAM.
Las versiones Junos OS afectadas de Juniper Networks son:
14.1 desde 14.1R5 antes de 14.1R8-S4, 14.1R9;
14.1X53 antes de 14.1X53-D46 en las series EX y QFX;
14.2 desde 14.2R3 antes de 14.2R7-S8, 14.2R8;
Ninguna otra publicación de Junos OS se ve afectada por este problema.
Ningún otro producto de Juniper Networks se ve afectado por este problema.

Solución:

Las siguientes versiones de software se han actualizado para resolver este problema específico: Junos 14.1R8-S4, 14.1R9, 14.1X53-D46, 14.2R7-S8, 14.2R8 y todas las versiones posteriores.

FUENTES:

Juniper. (Octubre 2017). Junos: Potential remote code execution vulnerability in PAM (CVE-2017-10615). Octubre 2017, de Juniper Sitio web: https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10818&cat=SIRT_1&actp=LIST

VULNERABILIDAD DE ESCALAMIENTO DE PRIVILEGIOS DE MOTOR DE CISCO IDENTITY SERVICES

Criticidad: Alta
Impacto: Escalación de Privilegios
Vulnerabilidad:
Ejecución: Remota
Plataforma(s):
afectada(s): Cisco Identity Services Engine (ISE) 1.4, 2.0, 2.0.1, 2.1.0
Referencia: CVE-2017-12261

Descripción:

Una vulnerabilidad en el shell restringido del Cisco Identity Services Engine (ISE) al que se puede acceder a través de SSH podría permitir que un atacante local autenticado ejecute comandos CLI arbitrarios con privilegios elevados.

La vulnerabilidad se debe a la validación de entrada incompleta de la entrada del usuario para los comandos CLI emitidos en el shell restringido. Un atacante podría aprovechar esta vulnerabilidad al autenticarse en el dispositivo de destino y ejecutar comandos que podrían derivar en privilegios elevados. Un atacante necesitaría credenciales de usuario válidas para el dispositivo a fin de aprovechar esta vulnerabilidad.

Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. No hay soluciones alternativas que solucionen esta vulnerabilidad.

FUENTES:

Seguridad de Cisco. (Noviembre 2017). Vulnerabilidad de escalamiento de privilegios de motor de Cisco Identity Services. Noviembre 2017, de Cisco Sitio web: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-ise

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD DE INYECCIÓN DEL COMANDO DE LICENCIA INTELIGENTE DEL DISPOSITIVO DE SEGURIDAD CISCO FIREPOWER 4100 SERIES NGFW Y FIREPOWER 9300

Criticidad: Alta
Impacto: Inyección de Código
Vulnerabilidad:
Ejecución: Remota
Plataforma(s) afectada(s): Cisco Firepower Security que ejecutan los trenes de código FX-OS 1.1.3, 1.1.4 y 2.0.1.
Referencia: CVE-2017-12277

Descripción:

Una vulnerabilidad en el servicio Smart Licensing Manager del cortafuegos de próxima generación Cisco Firepower serie 4100 (NGFW) y el dispositivo de seguridad Firepower 9300 podría permitir a un atacante autenticado y remoto inyectar comandos arbitrarios que podrían ejecutarse con privilegios de administrador.

La vulnerabilidad se debe a una validación de entrada insuficiente de ciertos parámetros de configuración de Smart Licensing. Un atacante autenticado podría explotar la vulnerabilidad configurando una URL maliciosa dentro de la característica afectada. Un exploit exitoso podría permitir al atacante ejecutar comandos arbitrarios con privilegios de root.
Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. No hay soluciones alternativas que solucionen esta vulnerabilidad.

FUENTES:

Seguridad de Cisco. (Noviembre 2017). Vulnerabilidad de inyección del comando de licencia inteligente del dispositivo de seguridad Cisco Firepower 4100 Series NGFW y Firepower 9300. Noviembre 2017, de Cisco Sitio web: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-fpwr

VULNERABILIDAD DE INYECCIÓN SQL AUTENTICADA DE APROVISIONAMIENTO DE CISCO PRIME COLLABORATION

Criticidad: Alta
Impacto: Inyección de Código SQL
Vulnerabilidad:
Ejecución: Remota
Plataforma(s) afectada(s): Cisco Prime Collaboration anteriores a la 12.3.
Referencia: CVE-2017-12276

Descripción:

Una vulnerabilidad en el código del marco web para la interfaz de la base de datos SQL de la aplicación Cisco Prime Collaboration Provisioning podría permitir que un atacante remoto autenticado impacte la confidencialidad y la integridad de la aplicación mediante la ejecución de consultas SQL arbitrarias. El atacante podría leer o escribir información de la base de datos SQL.

La vulnerabilidad se debe a la falta de una validación adecuada en la entrada proporcionada por el usuario dentro de las consultas SQL. Un atacante podría aprovechar esta vulnerabilidad enviando URL creadas que contengan declaraciones SQL maliciosas a la aplicación afectada. Un exploit podría permitir al atacante determinar la presencia de ciertos valores y escribir entradas maliciosas en la base de datos SQL. El atacante necesitaría tener credenciales de usuario válidas.

Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. No hay soluciones alternativas que solucionen esta vulnerabilidad.

FUENTES:

Seguridad de Cisco. (Noviembre 2017). Vulnerabilidad de inyección SQL autenticada de aprovisionamiento de Cisco Prime Collaboration Alto. Noviembre 2017, de Cisco Sitio web: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-cpcp

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD DE ACCESO NO AUTORIZADO DEL MÓDULO ENTERPRISE CONTROLLER DE LA INFRAESTRUCTURA DE POLÍTICAS DE CISCO

Criticidad: Alta
Impacto: Acceso no Autorizado
Vulnerabilidad:
Ejecución: Remota
Plataforma(s) afectada(s): Cisco Application Policy Infrastructure Controller antes de la versión 1.5.
Referencia: CVE-2017-12262

Descripción:

Una vulnerabilidad dentro de la configuración de cortafuegos del Módulo Enterprise Controller de Infraestructura de Políticas de Aplicaciones de Cisco (APIC-EM) podría permitir que un atacante adyacente no autenticado obtenga acceso privilegiado a los servicios solo disponibles en la red interna del dispositivo.
La vulnerabilidad se debe a una regla de firewall incorrecta en el dispositivo. La configuración incorrecta podría permitir que el tráfico enviado a la interfaz pública del dispositivo se reenvíe a la red virtual interna del APIC-EM. Un atacante que sea lógicamente adyacente a la red en la que reside la interfaz pública del APIC-EM afectado podría aprovechar este comportamiento para obtener acceso a los servicios que escuchan en la red interna con privilegios elevados.

Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. No hay soluciones alternativas que solucionen esta vulnerabilidad.

FUENTES:

Seguridad de Cisco. (Noviembre 2017). Vulnerabilidad de acceso no autorizado del módulo Enterprise Controller de la infraestructura de políticas de Cisco. Noviembre, de Cisco Sitio web: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-apicem

VULNERABILIDAD DE DENEGACIÓN DE SERVICIO DEL PROTOCOLO DE CONSULTA DE RED DE ACCESO DE CISCO WIRELESS CONTROLLER

Criticidad: Media
Impacto: Denegación de Servicio
Vulnerabilidad:
Ejecución: Remota
Plataforma(s) afectada(s): controladores LAN inalámbricos de Cisco que ejecutan una versión vulnerable del software Cisco WLC
Referencia: CVE-2017-12282

Descripción:

Una vulnerabilidad en la funcionalidad de procesamiento de marcos de acceso de Access Network Query Protocol de los Controladores LAN inalámbricos de Cisco podría permitir que un atacante adyacente a RF de Capa 2 no autenticado ocasione que un dispositivo afectado se reinicie de forma inesperada, dando como resultado una condición de denegación de servicio (DoS).

La vulnerabilidad se debe a la validación incompleta de entrada de marcos de consulta ANQP por parte del dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad enviando un marco de consulta ANQP malformado a un dispositivo afectado que se encuentre en una red adyacente a RF. Un exploit exitoso podría permitir al atacante provocar que el dispositivo afectado se reinicie inesperadamente, lo que da como resultado una condición DoS.

No hay soluciones alternativas que solucionen esta vulnerabilidad.

FUENTES:

Seguridad de Cisco. (Noviembre 2017). Vulnerabilidad de denegación de servicio del protocolo de consulta de red de acceso de Cisco Wireless Controller. Noviembre 2017, de Cisco Sitio web: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171101-wlc4