SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]

AÑO 01 EDICIÓN 2.97

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)

•Keylogger: Software de vigilancia, el cual cuenta con la capacidad de grabar cada tecla pulsada en el sistema en un archivo, usualmente cifrado.

•BSOD: Blue Screen Of Death, “pantalla azul de la muerte”; se refiere a la pantalla mostrada por el sistema operativo de Windows cuando éste no puede recuperarse de un error del sistema.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD DE ACCESO AL SHELL DE DESARROLLO DE PUNTOS DE ACCESO DE LA SERIE CISCO AIRONET

Criticidad: *Alta*
Impacto: *Acceso no autorizado*
Vulnerabilidad:
Ejecución: *Local*
Plataforma(s) Afectada(s):
Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión de software vulnerable:

- *Aironet 1540 Series APs 1*
- *Aironet 1560 Series APs 2*
- *Aironet 1800 Series APs 3*
- *Aironet 2800 Series APs*
- *Aironet 3800 Series APs*

Referencia: *CVE-2019-1654*
Descripción:
Una vulnerabilidad en la autenticación de shell de desarrollo (devshell) para los puntos de acceso (AP) de la serie Cisco Aironet que ejecutan el sistema operativo Cisco AP-COS podría permitir que un atacante local autenticado accediera a la shell de desarrollo sin la autenticación adecuada, lo que permite el acceso de root al Linux subyacente OS. El atacante necesitaría credenciales de dispositivo válidas.

La vulnerabilidad se debe a que el software valida incorrectamente la entrada suministrada por el usuario en la solicitud de autenticación de CLI para el acceso de shell de desarrollo. Un atacante podría aprovechar esta vulnerabilidad al autenticarse en el dispositivo e ingresar una entrada diseñada en la CLI. Una explotación exitosa podría permitir al atacante acceder al shell de desarrollo de AP sin la autenticación adecuada, lo que permite el acceso de root al sistema operativo Linux subyacente.

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

FUENTES:

Vulnerabilidad de acceso al shell de desarrollo de puntos de acceso de la serie Cisco Aironet. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-aironet-shell

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDADES DE EJECUCIÓN REMOTA DE CÓDIGO SNMP EN CISCO IOS E IOS XE

Criticidad: *Alta*
Impacto: *Ejecución de código*
Vulnerabilidad:
Ejecución: *Remota*
Plataforma(s)
Afectada(s):
Estas vulnerabilidades afectan a todas las versiones del software Cisco IOS e IOS XE anteriores a la primera versión fija y afectan a todas las versiones de SNMP: versiones 1, 2c y 3.

Los dispositivos configurados con cualquiera de los siguientes MIB son vulnerables:

- *ADSL-LINE-MIB*
- *ALPS-MIB*
- *CISCO-ADSL-DMT-LINE-MIB*
- *CISCO-BSTUN-MIB*
- *CISCO-MAC-AUTH-BYPASS-MIB*
- *CISCO-SLB-EXT-MIB*
- *CISCO-VOZ-DNIS-MIB*
- *CISCO-VOZ-NÚMERO-EXPANSIÓN-MIB*
- *TN3270E-RT-MIB*

Referencia: *CVE-2017-6736,CVE-2017-6737,CVE-2017-6738*

Descripción:
El subsistema del Protocolo simple de administración de red (SNMP) del software Cisco IOS e IOS XE contiene múltiples vulnerabilidades que podrían permitir que un atacante remoto autenticado ejecute el código de forma remota en un sistema afectado o que un sistema afectado se vuelva a cargar. Un atacante podría explotar estas vulnerabilidades enviando un paquete SNMP diseñado a un sistema afectado a través de IPv4 o IPv6. Solo el tráfico dirigido a un sistema afectado puede usarse para explotar estas vulnerabilidades.

Las vulnerabilidades se deben a una condición de desbordamiento del búfer en el subsistema SNMP del software afectado. Las vulnerabilidades afectan a todas las versiones de SNMP - Versiones 1, 2c y 3. Para explotar estas vulnerabilidades a través de SNMP Versión 2c o anterior, el atacante debe conocer la cadena de comunidad de solo lectura de SNMP para el sistema afectado. Para explotar estas vulnerabilidades a través de la versión 3 de SNMP, el atacante debe tener credenciales de usuario para el sistema afectado. Un ataque exitoso podría permitir al atacante ejecutar código arbitrario y obtener el control total del sistema afectado o hacer que el sistema afectado se vuelva a cargar.

Se aconseja a los clientes que apliquen la solución provisional que se encuentra en la sección Soluciones provisionales a continuación. La información del software fijo está disponible a través del Cisco IOS Software Checker. Todos los dispositivos que hayan habilitado SNMP y no hayan excluido explícitamente las MIB u OID afectadas deben considerarse vulnerables.
Cisco ha lanzado actualizaciones de software que abordan estas vulnerabilidades. Hay soluciones que abordan estas vulnerabilidades.

FUENTES:

Vulnerabilidades de ejecución remota de código SNMP en Cisco IOS y IOS XE Software. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

LAS CREDENCIALES CODIFICADAS DE GRPC PUEDEN PERMITIR EL ACCESO NO AUTORIZADO A LOS SISTEMAS CON JUNOS NETWORK AGENT INSTALADO

Criticidad: *Bajo*
Impacto:
Vulnerabilidad:
Ejecución: *Remota*
Plataforma(s)
Afectada(s):
Este problema afecta a Junos OS 16.1, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3.:

Referencia: *(CVE-2019-0034)*

Descripción:
Investigaciones posteriores han determinado que este problema no tiene impacto. Si bien las credenciales existen en las versiones afectadas, no hay manera de explotar este problema, e incluso si el problema fuera explotable, no habría impacto. Estas credenciales existían para fines específicos de prueba de productos internos que no se utilizan como parte de las versiones de producción de Junos OS.

A partir de la versión 16.1R3 de Junos OS, la interfaz de telemetría de Junos admite llamadas a procedimientos remotos de gRPC de Google para aprovisionar sensores y suscribirse y recibir datos de telemetría.

Se encontró que los archivos de configuración utilizados por gRPC contenían credenciales codificadas que Junos Network Agent podría usar para realizar la lectura no autorizada de cierta información no crítica (por ejemplo, datos del sensor).

Además, las API expuestas a través del kit de herramientas de extensión de Juniper (JET) pueden ser capaces de realizar operaciones de "conjuntos" no críticos en el dispositivo. Estas API necesitan la autenticación del cliente para el cual se puede usar el nombre de usuario / contraseña.
La explotación exitosa de esta vulnerabilidad solo puede ocurrir si el paquete Junos Network Agent (Junos Telemetry Interface) está instalado en el dispositivo.

Solución:
Deshabilite el servicio gRPC a través del siguiente comando si no es necesario en su entorno:
delete system services extension-service request-response grpc
Además de la recomendación mencionada anteriormente, es una buena práctica de seguridad limitar la superficie de ataque explotable de los equipos de redes de infraestructura crítica. Use listas de acceso o filtros de firewall para limitar el acceso al dispositivo solo desde redes o hosts administrativos y de confianza.

FUENTES:

Las credenciales codificadas de gRPC pueden permitir el acceso no autorizado a los sistemas con Junos Network Agent instalado): https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10923&cat=SIRT_1&actp=LIST

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD EN EL CRUCE DE DIRECTORIOS DE TREND MICRO APEX ONE, OFFICESCAN Y WORRY-FREE BUSINESS SECURITY

Criticidad: *Alta*
Impacto: *Modificación de algunos archivos del sistema o información*
Vulnerabilidad: *Cruce de directorios*
Plataforma(s) Afectada(s):

- *Apex One B1066 hacía abajo*
- *OfficeScan XG Version 12.0*
- *OfficeScan 11.0SP1*
- *Worry-Free Business Security 10.0, 9.5 y 9.0 SP3*

Referencia: *CVE-2019-9489*

Descripción:

Una vulnerabilidad de directorio transversal podría permitir a un atacante modificar archivos arbitrarios en la consola de administración del producto afectado.

Solución:

Trend Micro ha lanzado nuevos parches críticos (CP) para Apex One, OfficeScan XG, OfficeScan 11.0 SP1 y Worry-Free Business Security versiones 9.0 SP3, 9.5 y 10. Estas PC resuelven una vulnerabilidad de cruce de directorios que podría permitir la modificación de un posible atacante archivos arbitrarios en las consolas Apex One, OfficeScan o Worry-Free.

FUENTES:

Vulnerabilidad en el cruce de directorios de Trend Micro Apex One, OfficeScan y Worry-Free Business Security: https://success.trendmicro.com/solution/1122250 20190306-nxos-file-access

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

HACKEO EN WIPRO; LOS HACKERS USAN LOS SISTEMAS DE LA COMPAÑÍA PARA ATACAR A SUS PROPIOS CLIENTES

Acorde a expertos en análisis forense informático del Instituto Internacional de Seguridad Cibernética (IICS) Wipro se encuentra investigando algunos reportes que sugieren que sus sistemas de TI han sido hackeados; es posible que los sistemas comprometidos se estén empleando para lanzar ciberataques contra algunos de los clientes de esta compañía.

Los reportes indican que algunos de los clientes de la compañía de servicios de TI detectaron actividades maliciosas de reconocimiento de redes comunicándose directamente a las redes de Wipro. Se estima que al menos diez o doce compañías han sido afectadas.

Aunque Wipro tardó un poco en fijar postura respecto a este incidente, finalmente publicó un comunicado mencionando: "Nuestros procesos internos son en verdad sólidos y nuestros sistemas de seguridad son los más avanzados para prevenir y detectar diversos intentos de ciberataques".

Acorde a los especialistas en análisis forense informático, el ataque se habría originado en el servidor de correo electrónico de la compañía, por lo que Wipro ya prepara una nueva red email de uso privado. Por el momento, los usuarios potencialmente afectados están siendo informados de la situación. Portavoces de la compañía han mantenido comunicación sobre las actualizaciones más recientes sobre este incidente: "Derivado de una compleja campaña de phishing, hemos detectado actividad anómala en las cuentas de algunos empleados en nuestra red interna".

Los expertos en análisis forense informático mencionan que, en cuanto los equipos de seguridad de Wipro detectaron la actividad inusual, comenzaron un proceso de investigación, identificando a los usuarios potencialmente afectados e implementando las medidas de contención de incidentes pertinentes, mitigando el riesgo de propagación a otras partes de los sistemas de la compañía.

Los portavoces de la compañía agregan que Wipro está tratando de aprovechar su experiencia como líder en la implementación de las mejores prácticas de ciberseguridad en colaboración con una amplia gama de socios en la industria para seguir recopilando información y realizar actividades de monitoreo avanzado contra amenazas cibernéticas, protegiendo la integridad de los sistemas de la compañía.

FUENTES:

Noticias de seguridad Informatica. (2019). HACKEO EN WIPRO; LOS HACKERS USAN LOS SISTEMAS DE LA COMPAÑÍA PARA ATACAR A SUS PROPIOS CLIENTES. Abril 16, de Forense digital Sitio web: https://noticiasseguridad.com/seguridad-informatica/hackeo-en-wipro-los-hackers-usan-los-sistemas-de-la-compania-para-atacar-a-sus-propios-clientes/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

NUEVA VULNERABILIDAD DÍA CERO EN INTERNET EXPLORER PERMITIRÍA ROBO DE ARCHIVOS LOCALES

Internet Explorer no es precisamente el buscador más popular, y en definitiva este nuevo incidente de seguridad no le ayudará. Acorde a especialistas del curso de informática forense del Instituto Internacional de Seguridad Cibernética (IICS), ha sido descubierta una vulnerabilidad día cero en este buscador que hace que las computadoras con Windows sean vulnerables a los ataques de robo de archivos.

Acorde a los reportes, la vulnerabilidad se encuentra en el uso de archivos MHT de Internet Explorer cuando un usuario guarda una página web. La vulnerabilidad está en la apertura de archivos MHT. "Internet Explorer es vulnerable a un ataque de Entidad Externa XML si un usuario abre un archivo .MHT especialmente diseñado. Este inconveniente permitiría a un atacante extraer archivos locales y realizar un reconocimiento remoto de la versión de Program instalada en la máquina comprometida. Por ejemplo, enviar una solicitud c:\Python27\NEWS.txt podría devolver como respuesta información de la versión de ese programa".

Acorde a los expertos del curso de informática forense, una computadora sigue siendo vulnerable a este ataque aún si no emplea Internet Explorer como su navegador predeterminado, sólo se requiere que este programa esté instalado en la computadora y que el usuario abra un archivo MHT, pues el sistema Windows usa Internet Explorer para abrir los archivos MHT de forma predeterminada.

Los investigadores encargados de descubrir esta vulnerabilidad publicaron sus hallazgos, incluyendo una prueba de concepto de la explotación, en días recientes, además afirman que Microsoft está al tanto de este problema de seguridad. Al respecto, Microsoft declaró: "Una corrección para esta vulnerabilidad podría ser lanzada en el futuro; por el momento no serán publicadas actualizaciones para este incidente. El caso está cerrado", concluyó la compañía.

Aunque la compañía ha decidido no corregir esta vulnerabilidad día cero por el momento, es necesario destacar que el exploit publicado por los investigadores ha demostrado ser funcional en Internet Explorer 11 en sistemas Windows 10 y 7, mencionan los especialistas del curso de informática forense.

FUENTES

Noticias de seguridad Informatica. (2019). NUEVA VULNERABILIDAD DÍA CERO EN INTERNET EXPLORER PERMITIRÍA ROBO DE ARCHIVOS LOCALES. Abril 15, de Forense Digital Sitio web: https://noticiasseguridad.com/vulnerabilidades/nueva-vulnerabilidad-dia-cero-en-internet-explorer-permitiria-robo-de-archivos-locales/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

FACEBOOK RECOLECTÓ LOS CONTACTOS DE EMAIL DE 1,5 MILLONES DE USUARIOS SIN SU CONOCIMIENTO

Facebook admitió que recopiló hasta 1,5 millones de contactos de correo electrónico de usuarios sin su consentimiento, en lo que es el más reciente problema de privacidad que afecta a la empresa de tecnología.

La red social más grande del mundo dijo el miércoles por la noche que las listas de contactos de correo electrónico se habían subido "involuntariamente" a Facebook tras un cambio de diseño hace casi dos años, y la compañía está ahora en proceso para eliminarlos.

Facebook dijo que el problema comenzó hace tres años cuando realizó cambios en el proceso de verificación paso a paso que los usuarios realizan cuando se registran para una cuenta en la plataforma. Antes de esos cambios, los usuarios tenían la opción de cargar sus listas de contactos de correo electrónico al abrir una cuenta para ayudarles a encontrar amigos que ya estaban en Facebook.

Pero en mayo de 2016, Facebook eliminó el lenguaje que explicaba que las listas de contactos de los usuarios podían cargarse en los servidores de la compañía cuando se registraban para obtener una cuenta. Esto significó que en algunos casos las listas de contactos de correo electrónico de las personas se cargaron en Facebook sin su conocimiento o consentimiento.

Un portavoz de Facebook dijo el miércoles que la firma no se dio cuenta de que esto estaba sucediendo hasta abril de este año, cuando dejó de ofrecer la verificación de la contraseña de correo electrónico como una opción para las personas que se registraron en Facebook por primera vez. "Cuando observamos los pasos por los que pasaban las personas para verificar sus cuentas, descubrimos que en algunos casos los contactos de correo electrónico de las personas también se subían involuntariamente a Facebook cuando crearon su cuenta", agregó el portavoz.

La compañía dijo que las listas de contactos subidas por error no se habían compartido con nadie fuera de Facebook. La noticia fue reportada por primera vez por Business Insider el miércoles.

Ashkan Soltani, exdirector de tecnología de la Comisión Federal de Comercio, tuiteó el miércoles por la noche que creía que era "uno de los comportamientos de @facebook de mayor implicación legal hasta la fecha". "Confío en que los reguladores echarán un vistazo", dijo.

El incidente es el más reciente problema de privacidad de Facebook, que tiene más de 2.000 millones de usuarios a nivel mundial. En los últimos 18 meses, estos han incluido el escándalo de datos de Cambridge Analytica y la filtración de seguridad más grande en su historia.

El director ejecutivo Mark Zuckerberg ha respondido a las críticas prometiendo introducir medidas más centradas en la privacidad en la plataforma, como la mensajería cifrada y una mejor seguridad de los datos.

FUENTES:

Facebook recolectó los contactos de email de 1,5 millones de usuarios sin su conocimiento. (2019, 19 abril). Recuperado 20 abril, 2019, de https://cnnespanol.cnn.com/2019/04/18/facebook-recolecto-los-contactos-de-email-de-15-millones-de-usuarios-sin-su-conocimiento/