BOLETÍN DE CIBERSEGURIDAD

JUNIO 2022

ADV

ÍNDICE

NOTICIAS INTERNACIONALES

VULNERABILIDAD DÍA CERO DE EJECUCIÓN REMOTA DE CÓDIGO EN CONFLUENCE SERVER Y DATA CENTER

03/06/2022

ESPECIALISTAS EN SEGURIDAD INFORMÁTICA DE LA FIRMA VOLEXITY DESCUBRIERON UNA VULNERABILIDAD DE EJECUCIÓN REMOTA DE CÓDIGO

https://noticiasseguridad.com/vulnerabilidades/cve-2022-26134-vulnerabilidad-dia-cero-de-ejecucion-remota-de-codigo-en-confluence-server-y-data-center/

RESIDE EN LAS VERSIONES MÁS RECIENTES

Especialistas en seguridad informática de la firma Volexity descubrieron una vulnerabilidad de ejecución remota de código (RCE) que reside en las versiones más recientes y con parches completos de Atlassian Confluence Server. Identificada como CVE-2022-26134, la falla ya ha sido notificada a la compañía.

Los investigadores describen que esta es una falla día cero en Confluence Server y Data Center. Volexity no planea publicar su prueba de concepto (PoC), pues Atlassian no ha emitido un parche oficial. La falla fue descubierta cuando los investigadores identificaron actividad sospechosa en sus servidores Atlassian Confluence, pudiendo comprobar que el error existe debido a que un actor de amenazas lanzó un exploit RCE contra su infraestructura.

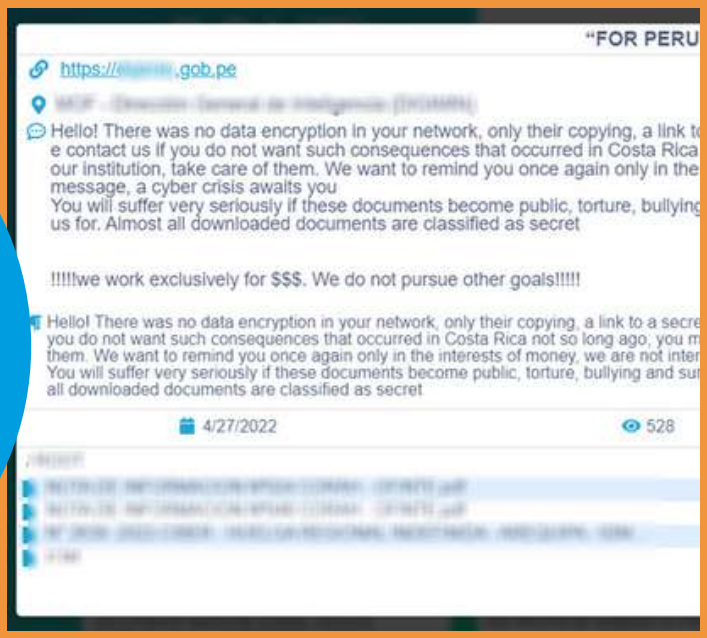
En las versiones afectadas de Confluence Server and Data Center, existe una vulnerabilidad de tipo “OGNL injection” que podría permitir que un atacante no autenticado ejecute código de forma arbitaria en el servidor Confluence o la instancia de Data Center.

Las versiones afectadas son desde la version 1.3.0 a 7.4.17, desde 7.13.0 a 7.13.7, 7.14.0 7.14.3, de 7.15.0 a 7.15.2, dedesde 7.16.0 a 7.16.4, desde 7.17.0 a 7.17.4, y desde 7.18.0 a 7.18.1.

HACKERS DEL RANSOMWARE CONTI ASEGURAN HABER INFECTADO SISTEMAS DE LA AGENCIA DE INTELIGENCIA DE PERÚ; 9 GB DE DATOS ROBADOS

27/05/2022

CONTI GROUP ATACARON A MIEMBROS DE LA DIRECCIÓN GENERAL DE INTELIGENCIA DEL MINISTERIO DEL INTERIOR



R. (2022c, mayo 17). Hackers rusos atacan al servicio de inteligencia peruano y exigen millonaria recompensa. RPP. https://rpp.pe/tecnologia/mas-tecnologia/hackers-rusos-atacan-al-servicio-de-inteligencia-peruano-y-exigen-millonaria-recompensa-noticia-1405437

HAN REVELADO EL SEGUIMIENTO A FUNCIONARIOS PÚBLICOS

Los reportes fueron dados por Sudaca, Hildebrant en sus Trece y La Encerrona, mostrando el proceder de Conti Group, atacantes que utilizan malware para secuestrar información malware para secuestrar información y pedir recompensas millonarias para no revelar la información.

Conti Group es uno de los grupos de ransomware más famosos del mundo y, a causa de sus actividades más recientes, ha estado en la mira de Estados Unidos por un devastador ataque a los sistemas informáticos del Gobierno de Costa Rica a fines del mes pasado. El Gobierno estadounidense anunció una recompensa de 10 millones de dólares por información de sus líderes.

¡En el caso del ataque a la entidad gubernamental de Perú, los atacantes publicaron también una invitación para que desde el organismo se comuniquen para llegar a un acuerdo. En el mensaje Conti también amenaza a Perú que puede ocurrir lo mismo que sucedió en Costa Rica.

Conti es un conocido grupo de ransomware que opera bajo la modalidad de ransomware-as-a-service desde 2019 y ha sido una de las bandas más prolíficas en el último año, con importantes organizaciones de distintas partes del mundo.

GOOGLE ADVIERTE SOBRE EL SPYWARE DE NIVEL EMPRESARIAL QUE SE DIRIGE A DISPOSITIVOS ANDROID E IOS

24/06/2022

LUEGO DE ANALIZAR 16 DE LOS 25 MÓDULOS CONOCIDOS, LOS INVESTIGADORES DE SEGURIDAD CIBERNÉTICA DE LOOKOUT CONCLUYERON QUE EL MALWARE INTENTA ROOTEAR LOS DISPOSITIVOS.

Mendoza, J. (2022, 24 junio). Google advierte sobre el spyware de nivel empresarial que se dirige a dispositivos Android e iOS. TekCrispy. https://www.tekcrispy.com/2022/06/24/google-spyware-android-ios/

EL SPYWARE, LLAMADO HERMIT, ES UN SOFTWARE DE VIGILANCIA MODULAR

Tiene características que incluyen: grabar audio, redirigir o hacer llamadas telefónicas, robar grandes cantidades de información como mensajes SMS, registros de llamadas, listas de contactos, fotos y extracción de datos de ubicación GPS.

Así funciona el Spyware en Android e iOS:

Esto es lo que se determinó en la muestra de Android que recolectó Lookout:

- La muestra de Android necesita que la víctima descargue una APK después de permitir la instalación de apps móviles de fuentes desconocidas. Aquí el malware se disfrazó como una aplicación de Samsung y utilizó Firebase para establecer su infraestructura de comando y control (C2).
- De acuerdo con los investigadores: “Si bien el APK en sí no contiene ningún exploit, el código sugiere la presencia de exploits que podrían descargarse y ejecutarse”.
-
- Google notificó a los usuarios de Android afectados por la aplicación. También realizó cambios en Google Play Protect para proteger a los usuarios de las actividades maliciosas. Además, deshabilitó los proyectos de Firebase asociados con el software espía.

ACTUALIZACIÓN APACHE HTTP SERVER 2.4.54 PARA CORREGIR MÚLTIPLES VULNERABILIDADES

20/06/2022

ESTA VERSIÓN DE APACHE ES UNA VERSIÓN DE SEGURIDAD, CARACTERÍSTICAS Y CORRECCIÓN DE ERRORES.

La Redacción. (2022, 20 junio). Apache HTTP Server 2.4.54 llega con 19 cambios y corrige 8 vulnerabilidades. laboratorio linux. https://laboratoriolinux.es/index.php/-noticias-mundo-linux-/software/32438-apache-http-server-2-4-54-llega-con-19-cambios-y-corrige-8-vulnerabilidades.html

APACHE HTTP SERVER 2.4.54, SIENDO ESTA VERSIÓN DE APACHE ES LA ÚLTIMA VERSIÓN GA

Hace poco la Apache Software Foundation y Apache HTTP Server Project dieron a conocer el lanzamiento de una nueva versión de Apache HTTP Server 2.4.54, siendo esta versión de Apache es la última versión GA de la rama de nueva generación 2.4.x de Apache HTTPD y representa quince años de innovación por parte del proyecto y que se recomienda sobre todas las versiones anteriores. Esta versión de Apache es una versión de seguridad, características y corrección de errores.

La nueva versión que se presenta introduce 19 cambios y corrige 8 vulnerabilidades, de las cuales algunas de ellas permitían el acceso a datos, tambien podían conducir a denegación del servicio, entre otras cosas más.

Cabe mencionar que esta versión requiere Apache Portable Runtime (APR), versión mínima 1.5.x, y APR-Util, versión mínima 1.5.x. Algunas funciones pueden requerir la versión 1.6.x de APR y APR-Util. Las bibliotecas APR deben actualizarse para que todas las funciones de httpd funcionen correctamente.

LITUANIA SUFRE CIBERATAQUES RUSOS EN RESPUESTA AL BLOQUEO DE KALININGRADO

27/06/2022

LITUANIA REGISTRÓ UN ELEVADO NÚMERO DE CIBERATAQUES CONTRA PÁGINAS WEB TANTO GUBERNAMENTALES

H. (2022, j 15). Reuniovelan una vulnerabilidad crítica en Windows que debe parchearse inmediatamente. HackWise. https://hackwise.mx/revelan-una-vulnerabilidad-critica-en-windows-que-debe-parchearse-inmediatamente/

Los ataques se produjeron después de que Lituania implementara hace una semana sanciones europeas que afectan el tránsito por ferrocarril de ciertos bienes desde Rusia al enclave ruso de Kaliningrado, en el oeste del país báltico.

Según medios locales, el grupo de hackers rusos Killnet realizó ataques de tipo DDOS (acrónimo de Distributed Denial of Service o denegación de servicio) contra una amplia gama de instituciones públicas, entre ellas el servicio de hacienda, el departamento de migración y la autoridad aeroportuaria lituana.

Killnet confirmó a través de su cuenta de Telegram que está detrás de los ataques.

El responsable del Centro Nacional de Ciberseguridad de Lituania, Jonas Skardinskas, declaró al portal informativo Delfi que es probable que la ofensiva continúe en los próximos días y afecte especialmente a los sectores del transporte, la energía y las finanzas.

La directora del departamento de migración de Lituania, Evelina Guzinskaité, afirmó según medios locales que el bloqueo de sus sistemas está llevando a que se produzcan retrasos en la expedición de pasaportes y permisos de residencia.

Las agencias de ciberseguridad de los países bálticos -Lituania, Letonia y Estonia- han informado de un aumento de la actividad hostil en el ciberespacio desde que Rusia invadió Ucrania el pasado mes de febrero.

FOLLINA: DOCUMENTOS DE MS OFFICE COMO VULNERABILIDAD

10/06/2022

NVESTIGADORES DEL LABORATORIO DE CIENCIAS DE LA COMPUTACIÓN E INTELIGENCIA ARTIFICIAL (CSAIL) DEL MIT DESCUBRIERON UN FALLO DE SEGURIDAD EN LOS CHIPS M1 DE APPLE.

Miranda, L. (2022, 10 junio). PACMAN: el ataque que vulnera la seguridad del Apple M1. Hipertextual. https://hipertextual.com/2022/06/pacman-apple-m1-ataque-vulnerabilidad-mit

ICreando un ataque mixto conocido como PACMAN, superaron la última línea de defensa del Apple Silicon sin ser detectados y no existe un parche de software que pueda solucionarlo.

El fallo se encuentra en el Código de Autenticación de Puntero (PAC), un mecanismo de seguridad que protege al sistema frente a vulnerabilidades de corrupción en la memoria. Esta tecnología asigna una firma criptográfica a los valores del puntero que se valida antes de utilizarlo. De este modo se evita que un atacante modifique los punteros para manipular objetos en el sistema o filtrar información privada.

Aunque la autenticación de puntero es eficiente para evitar que un atacante obtenga el control de un Mac con M1, no es una solución perfecta. La medida se implementó en ARM 8.3 y protege a los usuarios ante exploits que intentan engañar al dispositivo para que ejecute código malicioso. Al no contar con una clave para crear las firmas criptográficas, el hacker difícilmente creará punteros válidos.

NOTICIAS NACIONALES

ES MOMENTO QUE LAS PYMES PRIORICEN SU CIBERSEGURIDAD

30/06/2022

LAS PEQUEÑAS Y MEDIANAS EMPRESAS (PYMES) SE POSICIONAN COMO UNO DE LOS OBJETIVOS CLAVE DE LOS ATACANTES.

Golombek, J. B. (2022, 30 junio). Es momento que las PyMEs prioricen su ciberseguridad. El Sol de México | Noticias, Deportes, Gossip, Columnas. https://www.elsoldemexico.com.mx/analisis/es-momento-que-las-pymes-prioricen-su-ciberseguridad-8524272.html

En Kaspersky detectamos, en los primeros meses de este año, una tendencia al alza en ataques dirigidos a las PyMEs. Uno de ellos es el Troyano-PSW (Password Stealing Ware), malware que roba contraseñas y permite a los atacantes obtener acceso a la red corporativa y robar información confidencial. Desafortunadamente, México es el país de la región en el que se ha registrado el mayor número de detecciones de estos ataques con 323 mil 434 en 2022, 161.5% más que en 2021 cuando se reportaron 123 mil 640.

Otra herramienta que los ciberdelincuentes emplean contra este sector son los ataques a través de páginas web que redirigen a los usuarios hacia sitios que contienen exploits, un conjunto de programas maliciosos que tienen códigos ejecutables capaces de aprovecharse de una o más vulnerabilidades en el software local o remoto de la computadora. En este sentido, México se ubica en la cuarta posición con 619 mil detecciones, apenas por debajo de Brasil, Perú y Colombia.

Por otro lado, están los ataques a sistemas de Protocolo de escritorio remoto (RDP, por sus siglas en inglés), una tecnología que fue ampliamente adoptada a partir de la pandemia y que permite que las computadoras existentes en una misma red corporativa se conecten y accedan de forma remota. En ellos, los cibercriminales han visto una forma de acceder a toda una red empresarial. México ocupa el tercer lugar en este tipo de ataques con casi 5 millones de vulnerabilidades de este tipo.

MÉXICO DESTACA EN CIBERSEGURIDAD: BANXICO

20/06/2022

MÉXICO ESTÁ ENTRE LOS PAÍSES MEJOR PREPARADOS PARA HACER FRENTE A LOS RETOS DE CIBERATAQUES CON BASE EN EL ÍNDICE GLOBAL DE CIBERSEGURIDAD (IGC) DE LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (ITU)

Reynold, V. (2022, 20 junio). México destaca en ciberseguridad: Banxico. El Heraldo de México. https://heraldodemexico.com.mx/economia/2022/6/20/mexico-destaca-en-ciberseguridad-banxico-414994.html

Así, el país tiene un índice de 81.68 puntos, por encima de la media y la calificación lo coloca en la clasificación 61 de 194 naciones, destacó Banxico en el reporte.

Banxico refirió que según lo indicado por la ITU, México presenta fortalezas en las medidas de cooperación y técnicas; y en las organizacionales, son área de oportunidad.

Con respecto a 2018, México tuvo un incremento de 29.8 por ciento, frente al alza promedio en la calificación del IGC de 9.5 por ciento.

En tanto, el Índice de Riesgo de Ciberataques Financieros, que es estimado con base en una metodología del Fondo Monetario Internacional (FMI), mide el riesgo cibernético en el sector para distintos países con base en noticias de periódicos internacionales.

Así, Banxico precisó que al aplicar la metodología del FMI con noticias de enero de 2017 a marzo de 2022, México está en la posición 39 de 105 países con una calificación de 3.68 por ciento.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: JUNIO 2022

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-31344	06/02/2022	Online Car Wash Booking System v1.0n	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-31344

Descripción: Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/classes/Master.php?f=delete_booking.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-26869	06/02/2022	Dell PowerStore versions 2.0.0.x, 2.0.1.x and 2.1.0.x	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-26869

Descripción: A remote unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure and arbitrary code execution.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-30493	06/27/2022	LFI unauthenticated	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-23167

Descripción: Attacker crafts a GET request to: /mobile/downloadfile.aspx? Filename =../../windows/boot.ini the LFI is UNAUTHENTICATED.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-30500	05/26/2022	Vulnerabilidad inyección SQL en Jfinal cms 5.1.0	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-30500

Descripción: Jfinal cms 5.1.0 is vulnerable to SQL Injection.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-29247	06/27/2022	Vulnerabilidad inyección SQL en Jfinal cms 5.1.0	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-29247

Descripción: Electron is a framework for writing cross-platform desktop applications using JavaScript (JS), HTML, and CSS. A vulnerability in versions prior to 18.0.0-beta.6, 17.2.0, 16.2.6, and 15.5.5 allows a renderer with JS execution to obtain access to a new renderer process with `nodeIntegrationInSubFrames

TABLA DE VULNERABILIDADES RELEVANTES: JUNIO 2022

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2021-35104	06/14/2022	Buffer overflow	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2021-35104

Descripción: Possible buffer overflow due to improper parsing of headers while playing the FLAC audio clip in Snapdragon Auto

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-32156	06/15/2022	TLS certifica	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-32156

Descripción: However, connections from misconfigured nodes without valid certificates did not fail by default. After updating to version 9.0, see Configure TLS host name validation for the Splunk CLI

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-29496	06/17/2022	A stack-based buffer overflow vulnerability exists.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-29496

Descripción: A stack-based buffer overflow vulnerability exists in the BlynkConsole.h runCommand functionality of Blynk -Library v1.0.1.

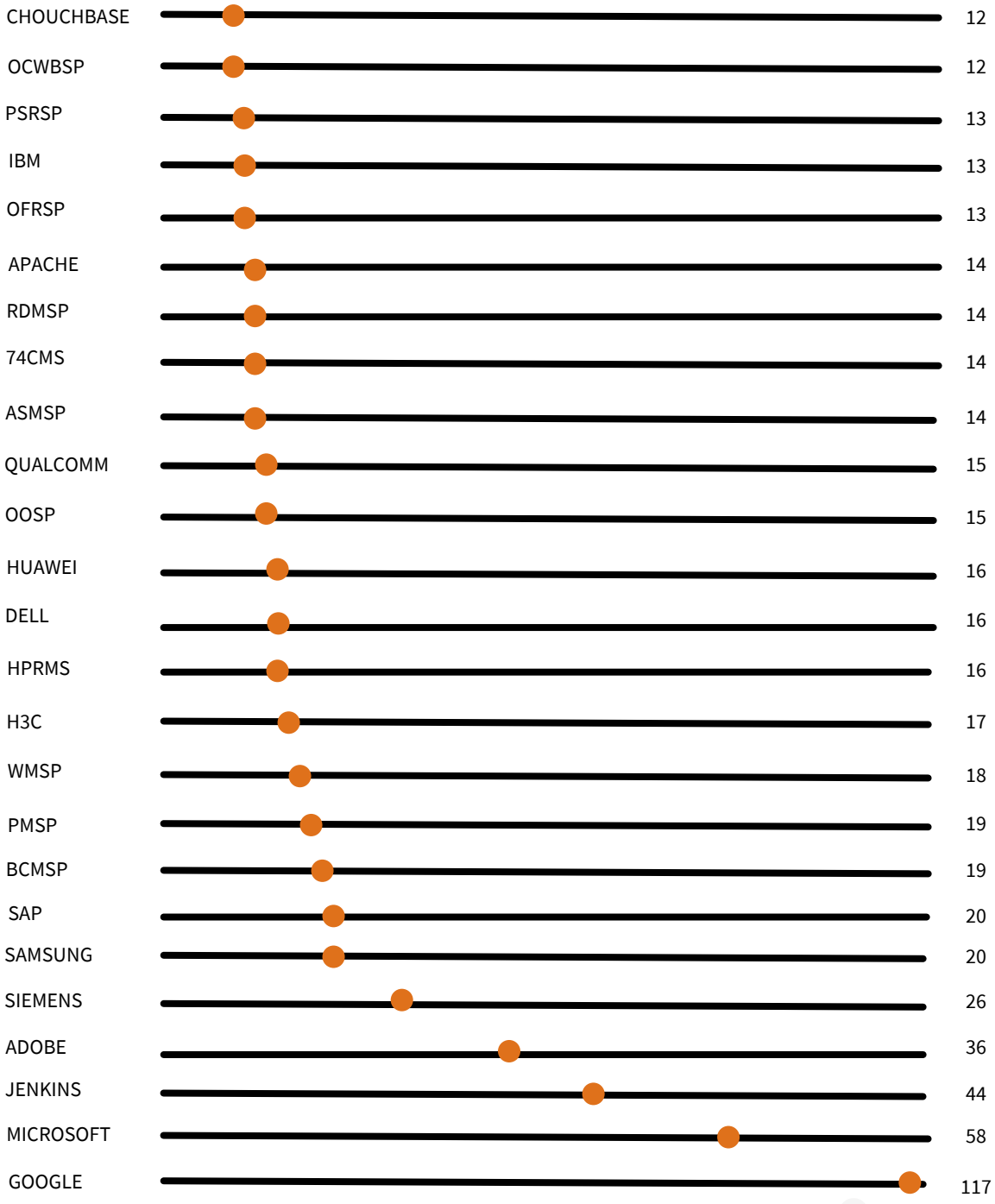
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-22318	06/21/2022	Invalid unauthenticated user	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-22318

Descripción: IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system.

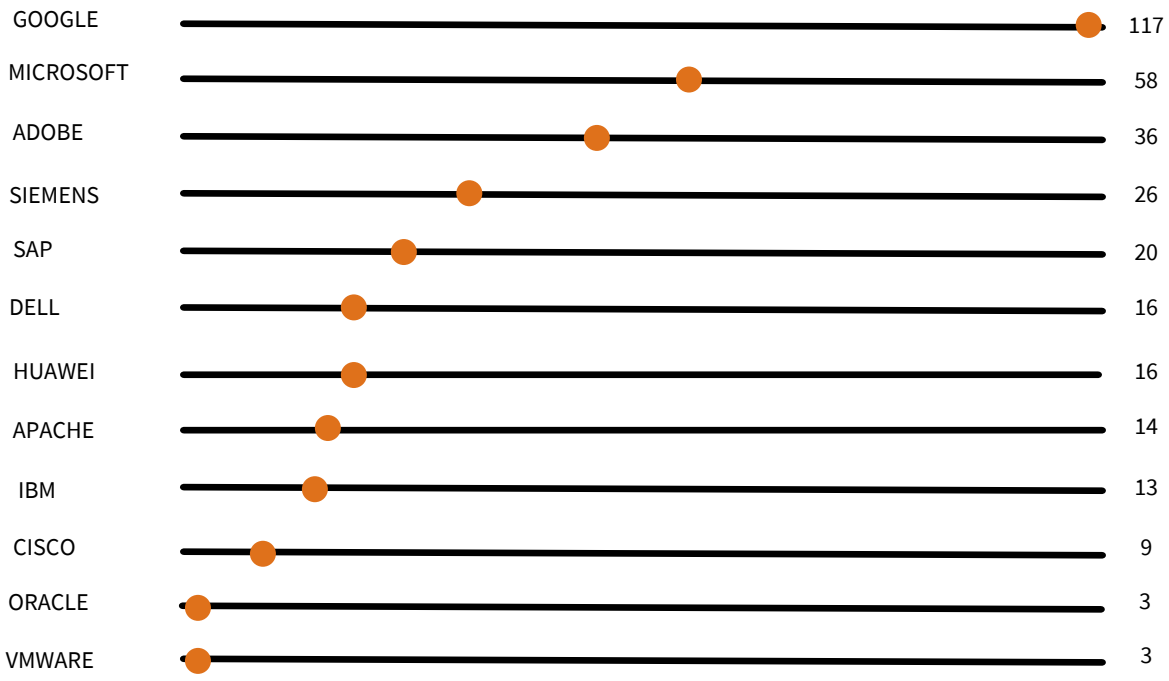
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-22980	06/23/2022	A Spring Data MongoDB application is vulnerable	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-22980

Descripción: A Spring Data MongoDB application is vulnerable to SpEL Injection when using @Query or @Aggregation-annotated query methods with SpEL expressions that contain query parameter placeholders for value binding if the input is not sanitized.

FABRICANTES Y SUS VULNERABILIDADES RELEVANTES: JUNIO DE 2022



EMPRESAS MULTINACIONALES Y SUS VULNERABILIDADES: JUNIO DE 2022



CULTURA DE CIBERSEGURIDAD

SPYWARE

¿QUÉ ES SPYWARE?

Software diseñado para recopilar datos de un ordenador u otro dispositivo y reenviarlos a un tercero sin el conocimiento o consentimiento del usuario. Esto a menudo incluye la recopilación de datos confidenciales (como contraseñas, números PIN e información de tarjetas), la supervisión de teclas, el rastreo de los hábitos de navegación y la recopilación de direcciones de correo electrónico entre otras.

CLASIFICACIONES PRINCIPALES

- **Spyware troyano:** infecta los ordenadores en forma de malware troyano.
- **Adware:** actúa como spyware para supervisar ordenadores y dispositivos.
- **Archivos de cookies:** rastreo en discos duros que rastrean a un usuario en Internet si un sitio es consciente de las cookies de rastreo y está diseñado para utilizarlas.
- **Supervisores de sistema:** Diseñados para supervisar cualquier actividad en un ordenador y capturar datos confidenciales, como pulsaciones de teclas, sitios visitados, correos electrónicos y mucho más.

EJEMPLOS DE SPYWARE

Con el desarrollo de las tecnologías de ciber seguridad a lo largo de los años, muchos programas de spyware han desaparecido, mientras que otros, algunas formas de spyware más sofisticadas han ido apareciendo. Algunos de los ejemplos más conocidos de spyware son los siguientes:

CoolWebSearch: Este programa aprovechaba las vulnerabilidades de la seguridad del Internet Explorer para secuestrar el navegador, cambiar los ajustes y enviar datos de búsqueda a su autor.

Gator: Normalmente alojado en los software de compartir archivos, como Kazaa, este programa controlaba los hábitos de navegación por internet de la víctima y usaba la información para mandar una selección de anuncios más adecuada.

Internet Optimizer: Especialmente popular en los tiempos de la conexión telefónica, este programa prometía mejorar la velocidad de internet. En lugar de eso, reemplazaba todas las páginas de error y páginas de registro con anuncios.

TIBS Dialer: Era un secuestrador de módem que desconectaba el ordenador de la víctima de la línea de teléfono de la red local y la conectaba a un número de pago diseñado para acceder a páginas de pornografía.

SPYWARE

Zlob: También conocido como Zlob Troyan, este programa usa vulnerabilidades en los códec de ActiveX para descargarse en el ordenador y registrar los historiales de búsquedas y navegación, así como las pulsaciones del teclado.

¿CÓMO ELIMINAR SPYWARE?

Lo puedes eliminar de forma manual entrando en el panel de control, aunque es un trabajo bastante lento y tedioso. También hay que tener en cuenta que es complicado encontrar un programa espía porque está hecho para que el propietario no se dé cuenta de que está instalado en tu ordenador.

Muchas veces las infecciones de virus se deben a brechas de seguridad de nuestro ordenador o dispositivos. Por eso es imprescindible, y de especial relevancia, mantener siempre actualizados el sistema operativo y todos los programas instalados.

ATT&CK puede ser útil para la inteligencia contra amenazas informáticas, ya que permite describir comportamientos adversarios de manera estándar. Se puede hacer un seguimiento de los actores con asociaciones respecto a las técnicas y tácticas en **ATT&CK**, que se sabe que utilizan. Tanto a nivel ofensivo, como defensivo, las matrices proporcionan gran información. A nivel ofensivo podrían utilizarse para acciones como:

- Tareas de pentesting.
- Equipos de Red team.
- Detección de comportamientos anómalos y búsqueda de amenazas (Threat Intelligence).
- Construcción de medidas a nivel defensivo.
- Mejora de equipos defensivos.

CONCLUSIÓN

El conocimiento sobre tácticas y técnicas de ataque en el sector industrial aporta un gran valor para la comunidad de expertos en material de ciberseguridad, tanto a nivel ofensivo como defensivo. Por ello, es importante que se siga trabajando en diferentes líneas a futuro para:

- Afinar más la descripción de las técnicas. Sectorizar, aún más si cabe, las tácticas y técnicas ya que, dependiendo del sector, en muchas ocasiones, tanto atacantes, como defensores se encuentran con protocolos y dispositivos diferentes.

- Aportar más medidas defensivas para la detección de algunas técnicas o para evitar la explotación de estas.

MITRE ATT&CK es una base de conocimiento accesible a nivel mundial basada en observaciones del mundo real. La base de conocimientos de **ATT&CK** se utiliza como base para el desarrollo de metodologías y modelos de amenazas específicos en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad.

Con la creación de **ATT&CK, MITRE** está cumpliendo su misión de resolver problemas para un mundo más seguro, uniendo a las comunidades para desarrollar una ciberseguridad más efectiva. **ATT&CK** está abierto y disponible para cualquier persona u organización para su uso sin cargo.

REFERENCIAS

REFERENCIAS

- https://noticiasseguridad.com/vulnerabilidades/cve-2022-26134-vulnerabilidad-dia-cero-de-ejecucion-remota-de-codigo-en-confluence-server-y-data-center/
- https://noticiasseguridad.com/vulnerabilidades/una-vulnerabilidad-critica-con-una-puntuacion-cve-de-9-8-afecta-a-fusion-middleware-a-varios-sistemas-de-oracle-e-incluso-a-la-nube-de-oracle-parche-inmediatamente/
- https://www.tekcrispy.com/2022/06/24/google-spyware-android-ios/
- https://laboratoriolinux.es/index.php/-noticias-mundo-linux-/software/32438-apache-http-server-2-4-54-llega-con-19-cambios-y-corrige-8-vulnerabilidades.html
- https://hackwise.mx/revelan-una-vulnerabilidad-critica-en-windows-que-debe-parchearse-inmediatamente/
- https://hipertextual.com/2022/06/pacman-apple-m1-ataque-vulnerabilidad-mit
- https://www.elsoldemexico.com.mx/analisis/es-momento-que-las-pymes-prioricen-su-ciberseguridad-8524272.html
- https://heraldodemexico.com.mx/economia/2022/6/20/mexico-destaca-en-ciberseguridad-banxico-414994.html

ZERU

Cybersecurity Services

Security Operation Center - SOC by

ADV

+52 55 6178 9397

contacto@adv-ic.com

Av. Melchor Ocampo 193, Torre Privanza, Piso 11 Oficina 11D
Colonia Veronica Anzures. Delegación Miguel Hidalgo CP 11300