BOLETÍN DE CIBERSEGURIDAD

SEPTIEMBRE 2022

ADV

ÍNDICE

NOTICIAS INTERNACIONALES

UBER SUFRE UN GIGANTESCO HACKEO: EL ATACANTE DICE TENER ACCESO A TODA LA INFORMACIÓN DE LA EMPRESA

16/09/2022

UN HACKER COMPROMETIÓ LA APLICACIÓN DE MENSAJERÍA SLACK DE UN EMPLEADO Y LA UTILIZÓ PARA ENVIAR UN MENSAJE A LOS TRABAJADORES DE UBER ANUNCIANDO QUE LA EMPRESA HABÍA SUFRIDO UNA VIOLACIÓN DE DATOS.

J., M. (2022, 16 septiembre). Uber sufre un ataque informático: un «hacker» de 18 años vulnera sus sistemas informáticos. Cinco Días. , de https://cincodias.elpais.com/cincodias/2022/09/16/companias/1663328711_079738.html

Según ha avanzado The New York Time, un hacker comprometió la aplicación de mensajería Slack de un empleado y la utilizó para enviar un mensaje a los trabajadores de Uber anunciando que la empresa había sufrido una violación de datos. Al parecer, el pirata informático pudo acceder posteriormente a otros sistemas internos, publicando una foto explícita en una página de información interna para los empleados, añadió el citado periódico.

El sistema Slack fue desconectado el jueves por la tarde por Uber después de que los empleados recibieran el mensaje del pirata informático: "Anuncio que soy un hacker y que Uber ha sufrido una violación". El mensaje añadía una lista de varias bases de datos internas que habían sido vulneradas.

El supuesto hacker habría logrado vulnerar los sistemas de Uber tras enviar un mensaje de texto a un empleado de la compañía afirmando que era una persona del equipo técnico de Uber. Dicho trabajador fue persuadido de que entregase una contraseña que permitió al pirata informático acceder a los servicios de la empresa.

STARBUCKS HACKEADO, DATOS DE 219,000 CLIENTES FILTRADOS

19/09/2022

STARBUCKS SINGAPUR ANUNCIÓ POR CORREO ELECTRÓNICO A SUS CLIENTES QUE HABÍA DESCUBIERTO UN ACCESO NO AUTORIZADO A DATOS DE CONTACTO COMO NOMBRE, SEXO, FECHA DE NACIMIENTO, NÚMERO DE TELÉFONO, DIRECCIÓN DE CORREO ELECTRÓNICO Y DIRECCIÓN POSTAL.

Rasmus, P. (2022, 19 septiembre). Starbucks hackeado, datos de 219,000 clientes filtrados. Diario Palestina Libération . , de https://www.palestinaliberation.com/starbucks-hackeado-datos-de-219000-clientes-filtrados

«Las autoridades pertinentes han sido detenidas y Starbucks Singapur está trabajando con ellas en este asunto».indica el correo electrónico.

La cadena de cafeterías dijo que fue informada de la violación de su base de datos de clientes el 13 de septiembre y destaca que ningún dato relacionado con las tarjetas bancarias se ve afectado por este hackeo, ya que la cadena no las almacena. Al mismo tiempo, Starbucks Singapur pide a sus clientes que cambien la contraseña de su cuenta.

El hacker afirma haber vendido ya una copia de los datos robados por $3500 y está listo para ofrecer al menos cuatro copias más a los compradores interesados. El motivo de esta limitación es mantener artificialmente alto el valor de los datos ofrecidos, ya que venderlos a muchos malos actores disminuiría su valor a medida que se lanzan múltiples ataques simultáneamente. Este enfoque aumenta el riesgo de que los clientes de Starbucks Singapur se conviertan en el objetivo de ataques de phishing, ingeniería social y estafas.

HACKEAN A LA CADENA HOTELERA HOLIDAY INN, LA CONTRASEÑA ERA 'QWERTY1234

21/09/2022

DURANTE 24 HORAS, IHG RESPONDIÓ A LAS QUEJAS EN REDES SOCIALES DICIENDO QUE SUS SISTEMAS ESTABAN “EN MANTENIMIENTO”.

Zavia, M. S. (2022, 21 septiembre). Hackean a la cadena hotelera Holiday Inn. La contraseña era «Qwerty1234». Gizmodo en Español. , de https://es.gizmodo.com/hackean-a-la-cadena-hotelera-holiday-inn-la-contrasena-1849560816

Los atacantes obtuvieron acceso a la red interna de IHG mediante ingeniería social, engañando a un empleado para que descargara un malware de un archivo adjunto de correo electrónico. Habían planeado un ransomware (secuestrar los datos de IHG con cifrado para pedir un rescate), pero la empresa logró aislar sus servidores antes de que pudieran implementarlo.

NUEVA BRECHA AFECTA AL GIGANTE SAMSUNG

6/09/2022

LA EMPRESA MULTINACIONAL SAMSUNG ADMITIÓ EL PASADO DÍA 2 DE SEPTIEMBRE HABER SIDO OBJETIVO DE UNA BRECHA DE SEGURIDAD.

Security Response Center | Support. (2022, 6 septiembre). Samsung US. , de https://www.samsung.com/us/support/securityresponsecenter/

De acuerdo con el comunicado emitido, a finales del mes de julio, un tercero no autorizado tuvo acceso a información de algunos sistemas de Samsung en Estados Unidos, quedando expuesta información personal de varios clientes.

Entre la información a la que se habría tenido acceso se encontraba: el nombre, información demográfica y de contacto, fecha de nacimiento, e información de registro del producto, no encontrándose entre esta información de números de la Seguridad Social ni de tarjetas de crédito.

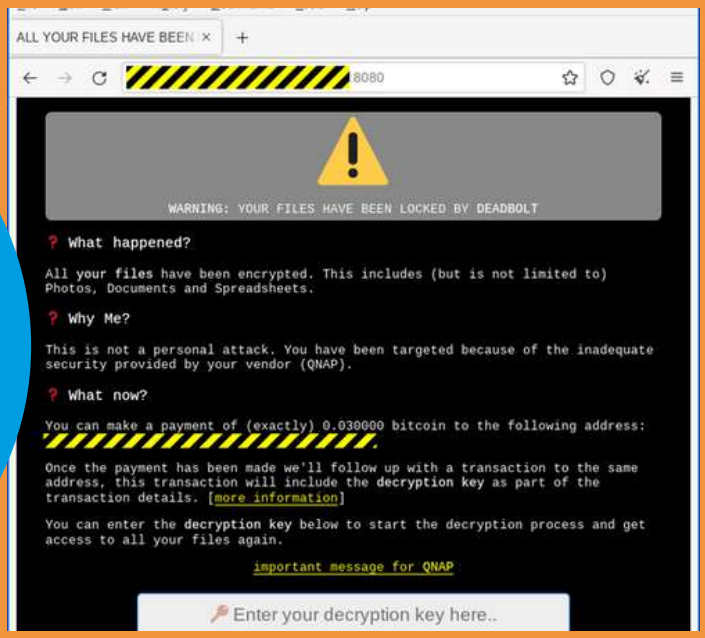
Este incidente es el segundo en menos de seis meses que se notifica, ya que en marzo se conoció que los datos internos del código fuente de sus smartphones fueron filtrados.

La compañía ha señalado que habría tomado medidas de seguridad al respecto para que no se vuelvan a repetir estos sucesos.

QNAP CORRIGE UN 0-DAY UTILIZADO EN NUEVOS ATAQUES DEL RANSOMWARE DEADBOLT

30/09/2022

ESTA SERÍA LA CUARTA OLEADA DE ATAQUES DE DEADBOLT DIRIGIDOS A APARATOS QNAP DESDE ENERO DE 2022, AL QUE SIGUIERON INCURSIONES SIMILARES EN MAYO Y JUNIO.



QNAP Systems, Inc. (s. f.). DeadBolt Ransomware - Security Advisory. QNAP Systems, Inc. - Network Attached Storage (NAS). , de https://www.qnap.com/en/security-advisory/qsa-22-24Nuevo

QNAP ha emitido un aviso de seguridad instando a los usuarios de sus NAS a que actualicen a la última versión de Photo Station.

Este aviso se produce tras detectar continuos ataques del ransomware DeadBolt que comenzaron el sábado y que estarían explotando una vulnerabilidad 0-day en Photo Station.

QNAP, que ya ha lanzado actualizaciones de seguridad para Photo Station, insta a sus clientes a actualizar este software a la última versión disponible y sugiere que los usuarios reemplacen Photo Station con QuMagie, una herramienta de administración de almacenamiento de fotos más segura para los dispositivos NAS de QNAP.

Los detalles de este fallo aún no están claros en este momento, pero desde la compañía recomiendan encarecidamente, para disminuir la posibilidad de ser atacado, que no se conecten los NAS de QNAP directamente a Internet y que se haga uso de la función myQNAPcloud Link proporcionada por QNAP, o que habiliten el servicio VPN.

Asimismo, recomiendan utilizar contraseñas seguras para las cuentas de usuario y realicen copias de seguridad periódicas para evitar la pérdida de datos.

MALWARE EN VMWARE ESXI CON CAPACIDADES BACKDOOR (UNC3886)

30/09/2022

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.

Un grupo de ciberespionaje desarrolla puertas traseras adaptadas a los hipervisores VMware ESXi. (2022, 3 octubre). IDG Communications S.A.U. , de https://cso.computerworld.es/cibercrimen/un-grupo-de-ciberespionaje-desarrolla-puertas-traseras-adaptadas-a-los-hipervisores-vmware-esxi

Se descubrió que los hackers están realizando implantes posteriores al compromiso nunca antes vistos en el software de virtualización de VMware, con el fin de tomar el control de los sistemas infectados y evadir la detección.

La división de inteligencia de amenazas Mandiant de Google, se refirió a esto como «un ecosistema de malware novedoso» que afecta a VMware ESXi, servidores Linux vCenter y máquinas virtuales de Windows, lo que permite a los atacantes mantener un acceso persistente al hipervisor y ejecutar comandos arbitrarios.

Los ataques de hyperjacking, según el proveedor de seguridad cibernética, implicaron el uso de paquetes de instalación de vSphere (VIB) maliciosos para infiltrar dos implantes, denominados VIRTUALPITA Y VIRTUALPIE, en los hipervisores ESXi

No hay evidencia de que se haya explotado una vulnerabilidad de día cero para obtener acceso a los servidores ESXi. Dicho esto, el uso de VIB troyanizados, un formato de paquete de software utilizado para facilitar la distribución de software y la gestión de máquinas virtuales, apunta a un nuevo nivel de sofisticación.

MICROSOFT CORRIGE DOS 0-DAY Y OTRAS 63 VULNERABILIDADES EN SU PATCH TUESDAY

30/09/2022

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.

Security Update Guide - Microsoft Security Response Center. (s. f.).de https://msrc.microsoft.com/update-guide/releaseNote/2022-Sep

Microsoft ha corregido, en su Patch Tuesday correspondiente al mes de septiembre, 63 vulnerabilidades entre las que se encuentran dos 0-day, uno de ellos activamente explotado y 5 fallos críticos que permitirían la ejecución remota de código.

El 0-day activamente explotado, identificado como CVE-2022-37969 y CVSS 7.8, fue descubierto por investigadores de DBAPPSecurity, Mandiant, CrowdStrike y Zscaler y afecta al sistema de archivos de registro común (CLFS), permitiendo que un atacante pueda obtener privilegios de sistema.

Por otro lado, el segundo 0-day que no ha sido explotado, se ha catalogado como CVE-2022-23960 y con CVSS 5.6, y hace referencia a una vulnerabilidad de restricción de especulación en la caché.

En cuanto a las vulnerabilidades críticas, 2 se encuentran en Microsoft Dynamics CRM (CVE-2022-35805 y CVE-2022-34700), otras 2 en IKE (CVE-2022-34722 y CVE-2022-34721) y, por último, un fallo en Windows TCP/IP (CVE-2022-34718), todos ellos permitirían la ejecución remota de código.

NOTICIAS NACIONALES

GUACAMAYA: EL GRUPO DE HACKERS QUE ATACÓ A LA SEDENA

3/10/2022

EN UNA PUBLICACIÓN DENTRO DEL SITIO ENLACE HACKTIVISTA, GUACAMAYA DESCRIBIÓ CON DETALLE LA FORMA EN LA QUE ACCEDIÓ A UN SERVIDOR DE LA SEDENA PARA ROBAR MILES DE ARCHIVOS Y CÓMO OTROS HACKERS TAMBIÉN DESCARGARON INFORMACIÓN

Riquelme, R. (2022, 3 octubre). Varios hackers ya habían infectado a la Sedena antes de Guacamaya. El Economista. , de https://www.eleconomista.com.mx/tecnologia/Varios-hackers-ya-habian-infectado-a-la-Sedena-antes-de-Guacamaya-20221003-0070.html

El grupo de hacktivistas Guacamaya usó un ataque contra la Secretaría de la Defensa Nacional (Sedena) que se diferencia de los que empleó contra otros ejércitos e instituciones latinoamericanas. El grupo de hackers explotó una vulnerabilidad en el servicio de correo electrónico Zimbra con la que extrajo los 6 terabytes de información del ejército mexicano y se dio cuenta de que otros ciberatacantes ya habían intentado descargar archivos desde sus servidores.

“Todas las demás filtraciones fueron descargadas con Proxyshell como se ve en el video, pero SEDENA fue con una vulnerabilidad antigua de Zimbra. Fue simplemente usar esto para explotar la vulnerabilidad y subir una webshell, y luego usar la webshell para descargar todos los correos de /opt/zimbra/store. Ya había muchas otras webshells allí, con fecha desde el 5 de Julio (la fecha puede ser fácilmente cambiado con touch -t pero también esta documentado que en Julio se empezó a explotar muchos servidores de Zimbra) y vimos que otros hackers también estuvieron descargando los correos a la vez”.

El grupo Guacamaya tardó alrededor de un mes desde que explotó la vulneración hasta que extrajo la información del servidor de la Sedena, de acuerdo con Hiram Camarillo, especialista en ciberseguridad de Seekurity, quien entabló comunicación con Guacamaya a través de Enlace Hacktivista.

Mientras que en un video publicado junto con sus declaraciones y un poema, donde revelaba la exfiltración de 6 terabytes de la Sedena, las hackers revelaban la forma en la que habían explotado el

grupo de tres vulnerabilidades Proxyshell para piratear la información de ejércitos como el chileno o el colombiano; en el caso de la Sedena, Guacamaya explotó las vulnerabilidades CVE-2022-27925 y CVE-2022-37042 del sistema de correo electrónico Zimbra

Mediante estas vulnerabilidades, de acuerdo con Camarillo, los hackers usaron una especie de programa espía, llamado webshell, que permite escribir código dentro del servidor infectado para acceder a la consola de comandos del mismo y desde ahí, comenzaron a descargar los archivos de la carpeta /opt/zimbra/store. Guacamaya se percató además de que otras webshells de otros hackers se encontraban dentro del servidor de la Sedena, al menos desde el 5 de julio de 2022.

Quiere decir que había varias personas dentro de ese servidor", dijo Camarillo.

Las vulnerabilidades de Zimbra fueron actualizadas en abril de 2022, luego de que la compañía liberó los parches correspondientes. Zimbra gestiona dos versiones disponibles de su herramienta colaborativa de correo electrónico: una gratuita de código abierto cuyo soporte es brindado por la comunidad y otra comercial en la que ofrece el soporte de la empresa.

CVE-2022-27925: Zimbra Collaboration (también conocido como ZCS) 8.8.15 y 9.0 tiene la funcionalidad mboximport que recibe un archivo ZIP y extrae archivos de él. Un usuario autenticado con derechos de administrador tiene la capacidad de cargar archivos arbitrarios en el sistema, lo que lleva al cruce de directorios. Este CVE inicial fue parcheado por Zimbra en marzo de 2022.
CVE-2022-37042: Zimbra Collaboration Suite (ZCS) 8.8.15 y 9.0 tiene la funcionalidad mboximport que recibe un archivo ZIP y extrae archivos de él. Al pasar por alto la autenticación (es decir, al no tener un token de autenticación), un atacante puede cargar archivos arbitrarios en el sistema, lo que lleva al cruce de directorios y la ejecución remota de código. NOTA: este problema existe debido a una solución incompleta para CVE-2022-27925, se solucionó el problema de autenticación en sus versiones 9.0.0P26 y 8.8.15P33 a fines de julio.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: SEPTIEMBRE 2022

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-41828	09/29/2022	Incorrect Type Conversion or Cast	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-41828

Descripción: In Amazon AWS Redshift JDBC Driver (aka amazon-redshift-jdbc-driver or redshift-jdbc42) before 2.1.0.8, the Object Factory does not check the class type when instantiating an object from a class name.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-29503	09/29/2022	Improper Restriction of Operations	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-29503

Descripción: A memory corruption vulnerability exists in the libpthread linuxthreads functionality of uClibC 0.9.33.2 and uClibC-ng 1.0.40. Thread allocation can lead to memory corruption. An attacker can create threads to trigger this vulnerability.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2021-45790	09/28/2022	Unrestricted Upload of File with Dangerous Type	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2021-45790

Descripción: An arbitrary file upload vulnerability was found in Metersphere v1.15.4. Unauthenticated users can upload any file to arbitrary directory, where attackers can write a cron job to execute commands.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2020-35674	09/28/2022	Improper Neutralization of Special Elements used in an SQL	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2020-35674

Descripción: BigProf Online Invoicing System before 2.9 suffers from an unauthenticated SQL Injection found in /membership_passwordReset.php (the endpoint that is responsible for issuing self-service password resets). An unauthenticated attacker is able to send a request containing a crafted payload that can result in sensitive information being extracted from the database, eventually leading into an application takeover. This vulnerability was introduced as a result of the developer trying to roll their own sanitization implementation in order to allow the application to be used in legacy environments.

TABLA DE VULNERABILIDADES RELEVANTES: SEPTIEMBRE 2022

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2020-27602	09/28/2022	Improper Neutralization of Special Elements	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2020-27602

Descripción: BigBlueButton before 2.2.7 does not have a protection mechanism for separator injection in meetingId, userId, and authToken.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2020-15332	09/28/2022	Cleartext Storage of Sensitive Information	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2020-15332

Descripción: Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has weak /opt/axess/etc/default/axess permissions.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2020-15331	09/28/2022	Missing Encryption of Sensitive Data	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2020-15331

Descripción: Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded OAUTH_SECRET_KEY in /opt/axess/etc/default/axess.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2016-2338	09/28/2022	Out-of-bounds Write	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2016-2338

Descripción: An exploitable heap overflow vulnerability exists in the Psych::Emitter start_document function of Ruby. In Psych::Emitter start_document function heap buffer "head" allocation is made based on tags array length. Specially constructed object passed as element of tags array can increase this array size after mentioned allocation and cause heap overflow.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-3332	09/28/2022	Improper Neutralization of Special Elements	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-3332

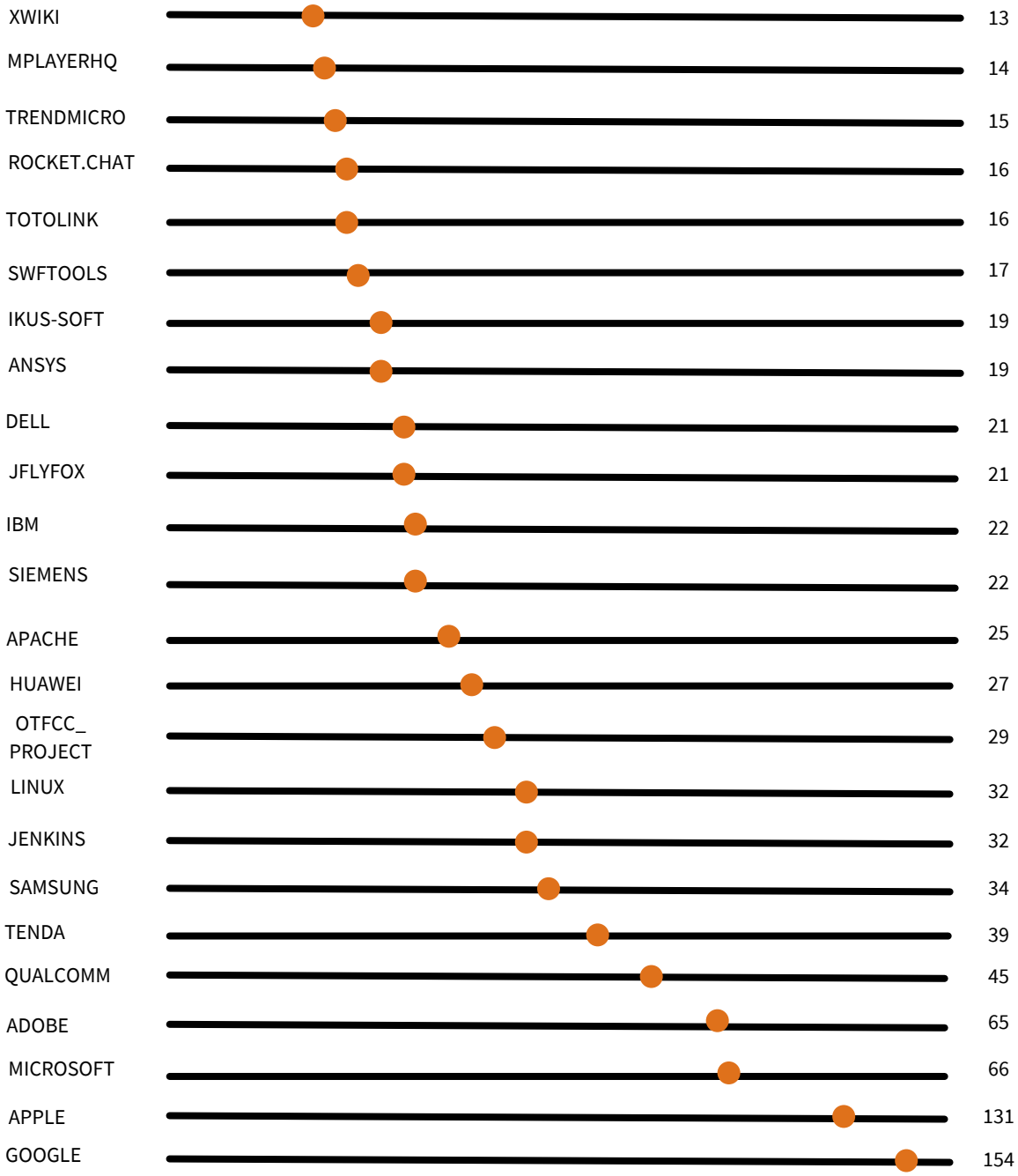
Descripción: https://nvd.nist.gov/vuln/detail/CVE-2022-3332

TABLA DE VULNERABILIDADES RELEVANTES: SEPTIEMBRE 2022

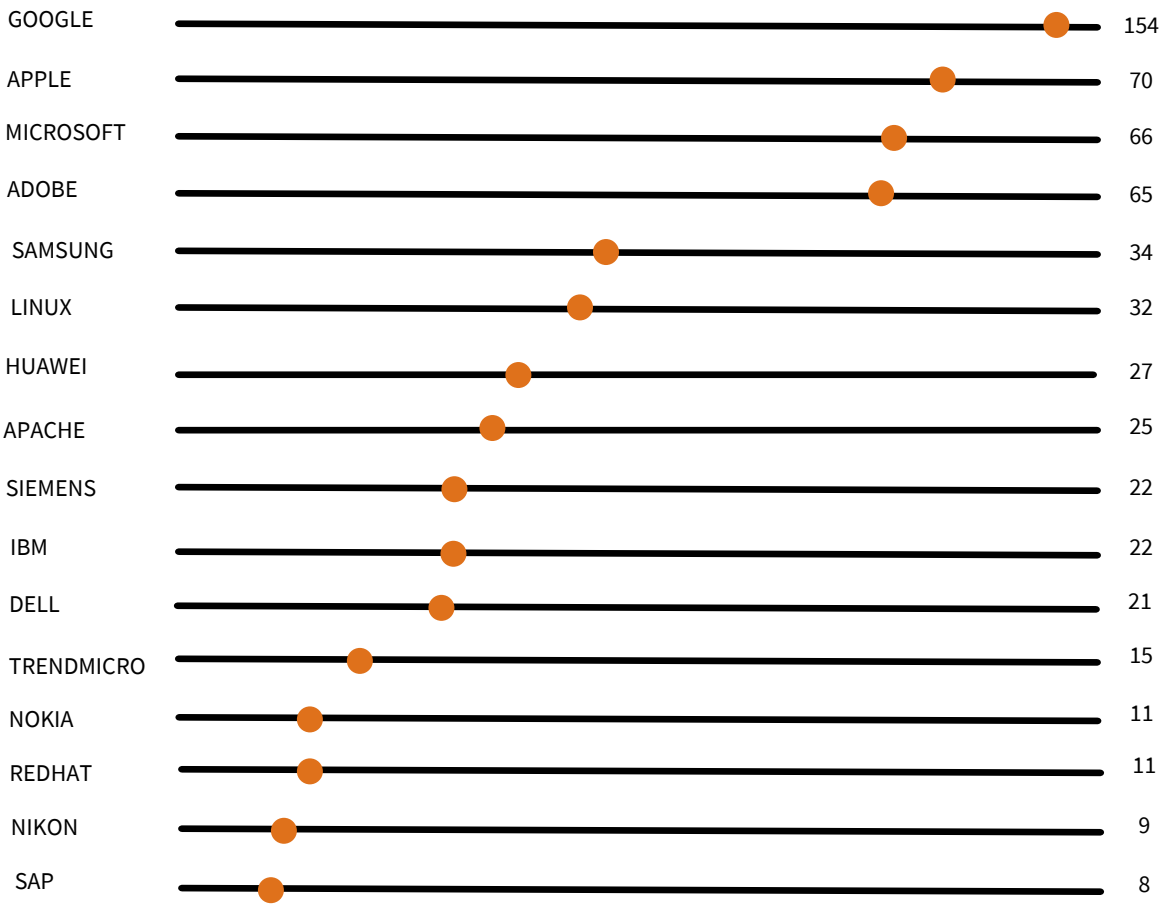
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-22522	09/28/2022	Use of Hard-coded Credentials	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-22522

Descripción: In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a remote, unauthenticated attacker could make use of hard-coded credentials to gain full access to the device.

FABRICANTES Y SUS VULNERABILIDADES RELEVANTES: SEPTIEMBRE DE 2022



EMPRESAS MULTINACIONALES Y SUS VULNERABILIDADES: SEPTIEMBRE DE 2022



CULTURA DE CIBERSEGURIDAD

SPYWARE

¿QUE ES SPYWARE?

Se define como un 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 y números de tarjetas de crédito), la supervisión de las pulsaciones de teclas, el rastreo de los hábitos de navegación y la recopilación de direcciones de correo electrónico.

Además de todo esto, estas actividades también afectan el rendimiento de la red, al ralentizar el sistema y afectar a todo el proceso empresarial. Generalmente se clasifican en cuatro categorías principales: troyanos, adware, cookies de rastreo y supervisores de sistema.

¿CÓMO EVITAR INFECTAR MI EQUIPO CON SPYWARE?

EVITA INSTALAR SOFTWARE GRATUITO DE FUENTES CUESTIONABLES

Hay muchas herramientas en línea que afirman realizar tareas que generalmente no puedes hacer con Windows o aplicaciones convencionales. Es posible que debas crear o completar un PDF, por ejemplo, y no tengas la herramienta comercial adecuada para hacerlo. O necesitas leer un formato de archivo poco conocido para un programa que no es de tu propiedad.

Una búsqueda en Google podría mostrar aplicaciones gratuitas que ofrecen hacer exactamente esas cosas. Si bien es posible que encuentres herramientas legítimas para realizar estas tareas, muchas de las opciones gratuitas pueden estar incluidas con software espía. Es mejor comprar una herramienta conocida por su reputación que arriesgarse con la alternativa.

UTILIZA SOFTWARE ANTI-MALWARE

Tu computadora debe estar protegida por algún tipo de software anti-malware o antivirus, y la mayoría de los programas modernos te protegerán del software espía común. Como mínimo, usa el software de seguridad integrado en Windows, aunque también puedes usar herramientas de terceros. Asegúrate de actualizar tu software constantemente.

MANTÉN TU COMPUTADORA ACTUALIZADA

Mantén su computadora actualizada con el último software de Windows y las actualizaciones de seguridad, o sigue estos pasos para solucionar problemas si tu computadora no se actualiza.

NO HAGAS CLIC EN NADA EN LO QUE NO CONFÍES

Sigue los consejos probados y verdaderos de nunca hacer clic en algo en lo que no confíes completamente. Eso incluye enlaces y archivos adjuntos en el correo electrónico; si no conoces al remitente o si la legitimidad del correo electrónico parece cuestionable, no abras nada dentro de él. Lo mismo es cierto para los enlaces siguientes en sitios web de calidad cuestionable.

REFERENCIAS

REFERENCIAS

- https://cincodias.elpais.com/cincodias/2022/09/16/companias/1663328711_079738.html
- https://www.palestinaliberation.com/starbucks-hackeado-datos-de-219000-clientes-filtrados
- https://es.gizmodo.com/hackean-a-la-cadena-hotelera-holiday-inn-la-contrasena-1849560816
- https://www.samsung.com/us/support/securityresponsecenter/
- https://www.qnap.com/en/security-advisory/qsa-22-24Nuevo
- https://cso.computerworld.es/cibercrimen/un-grupo-de-ciberespionaje-desarrolla-puertas-traseras-adaptadas-a-los-hipervisores-vmware-esxi
- https://msrc.microsoft.com/update-guide/releaseNote/2022-Sep
- https://www.eleconomista.com.mx/tecnologia/Varios-hackers-ya-habian-infectado-a-la-Sedena-antes-de-Guacamaya-20221003-0070.html
- https://latam.kaspersky.com/resource-center/threats/spyware

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