BOLETÍN DE CIBERSEGURIDAD

ABRIL 2022

ADV

ÍNDICE

NOTICIAS INTERNACIONALES

FBI DA A CONOCER EL CIERRE DE RAIDFORUMS Y LA DETENCIÓN DE SU ADMINISTRADOR DE 21 AÑOS

13/04/2022

EL ADMINISTRADOR Y FUNDADOR DE RAIDFORUMS, FUE ARRESTADO Y HA ESTADO BAJO CUSTODIA A LA ESPERA DE LA RESOLUCIÓN DE SU PROCESO DE EXTRADICIÓN.

El FBI hace oficial el cierre de RaidForums y la detención de su administrador de 21 años. (2021, 13 abril). elhacker.net. https://blog.elhacker.net/2022/04/el-fbi-hace-oficial-el-cierre-de-RaidForums-y-detieneadministrador-omnipotent-portugues-21-edad.html

DIOGO SANTOS COELHO DE PORTUGAL, FUE ARRESTADO

Conocido como Omnipotent, el administrador y fundador de RaidForums, Diogo Santos Coelho de Portugal, fue arrestado el 31 de enero en el Reino Unido y ha estado bajo custodia a la espera de la resolución de su proceso de extradición.

Se confirmó su detención y la de dos cómplices más del popular foro raidforums.com de ciberdelincuentes con una comunidad de más de medio millón de usuarios, el cual era bien conocido por tener a la venta vender el acceso a filtraciones de bases de datos de alto nivel pertenecientes a empresas de todos los sectores alrededor del mundo.

Éstas contenían información de millones de tarjetas de crédito, números de cuentas bancarias e información de rutas, así como los nombres de usuario y las contraseñas asociadas necesarias para acceder a las cuentas en línea.

Lo más sorprendente de todo es que el Departamento de Justicia de EE. UU. reconoce en su comunicado que Coelho tiene 21 años, por lo que únicamente tenía 14 años cuando lanzó RaidForums en 2015.

VULNERABILIDAD CRÍTICA EN JAVA PERMITE FALSIFICAR CERTIFICADOS, FIRMAS, MENSAJES WEBAUTHN Y EVADIR MECANISMOS DE AUTENTICACIÓN

28/04/2022

SE ACABA DE REVELAR UNA VULNERABILIDAD CRÍTICA QUE PUEDE FACILITAR QUE LOS ATACANTES FALSIFIQUEN CERTIFICADOS Y FIRMAS TLS.

Esta grave vulnerabilidad de Java permite falsificar certificados y firmas TLS. (2022, 28 abril).. HackWise. https://hackwise.mx/esta-grave-vulnerabilidad-de-java-permite-falsificar-certificados-y-firmas-tls/

PUEDEN FALSIFICAR MENSAJES DE AUTENTICACIÓN DE DOS FACTORES

La vulnerabilidad afecta la implementación del algoritmo de firma digital de curva elíptica (ECDSA por sus siglas en inglés) en las versiones de Java 15 y superiores. ECDSA es un algoritmo que utiliza los principios de la criptografía de curva elíptica para autenticar mensajes digitalmente. Una ventaja clave de ECDSA es el tamaño más pequeño de las claves que genera, en comparación con RSA u otros algoritmos criptográficos. Esto lo hace ideal para su uso en estándares que incluyen 2FA basado en FIDO, el Lenguaje de Marcado de Aserción de Seguridad, OpenID y JSON.

Toda clase de implementaciones Java podrían verse comprometidas si esta falla es explotada, incluyendo campos como las comunicaciones cifradas, tokens de autenticación, actualizaciones de código y otros. Oracle corrigió el error, identificado como CVE-202221449, en su código en su parche de seguridad trimestral.

Si bien al inicio Oracle había asignado a esta falla un puntaje de gravedad de 7.5/10, especialistas en ciberseguridad analizaron el reporte y concluyeron que la falla ameritaba una puntuación crítica de 10/10. Al respecto, el investigador Thomas Ptacek considera este reporte como el “error criptográfico del año”, dadas sus condiciones de explotación y problemas derivados del ataque.

SE DESCUBRIÓ UNA NUEVA VULNERABILIDAD EN EL NAVEGADOR CHROME, ZERO DAY. SOLUCIONADO

16/04/2022

SEGÚN UNA PUBLICACIÓN DE BLOG, GOOGLE SABE QUE EXISTE UN EXPLOIT PARA CVE-2022-1364. MIENTRAS SE EJECUTA, PUEDE BLOQUEAR CHROME O PERMITIR LA EJECUCIÓN DE CÓDIGO ARBITRARIO.

A. (2022a, abril 16). Google parchea el tercer día cero de Chrome explotado activamente de 2022. Posts US News ES. https://es.postsus.com/technology/208334.html

UNA VERSIÓN DE CHROME CONTIENE ALGUNAS VULNERABILIDADES,

La versión 100.0.4896.127 de Chrome contiene algunas vulnerabilidades, CVE-2022-1364, que se clasifica con gravedad “ALTA”. Esta es una “confusión de tipos en V8”, el motor WebAssembly y JavaScript de código abierto y alto rendimiento de Google. Según una publicación de blog, Google sabe que existe un exploit para CVE-2022-1364. Mientras se ejecuta, puede bloquear Chrome o permitir la ejecución de código arbitrario. Algo que no es para nada bueno con malas intenciones.

Eso significa que otros navegadores que se basan en el proyecto Chromium, incluidos Microsoft Edge y Vivaldi, también se ven afectados por CVE-2022-1364. Microsoft y Vivaldi reconocieron la vulnerabilidad y dijeron que actualizaron sus navegadores a la versión parcheada de Chromium.

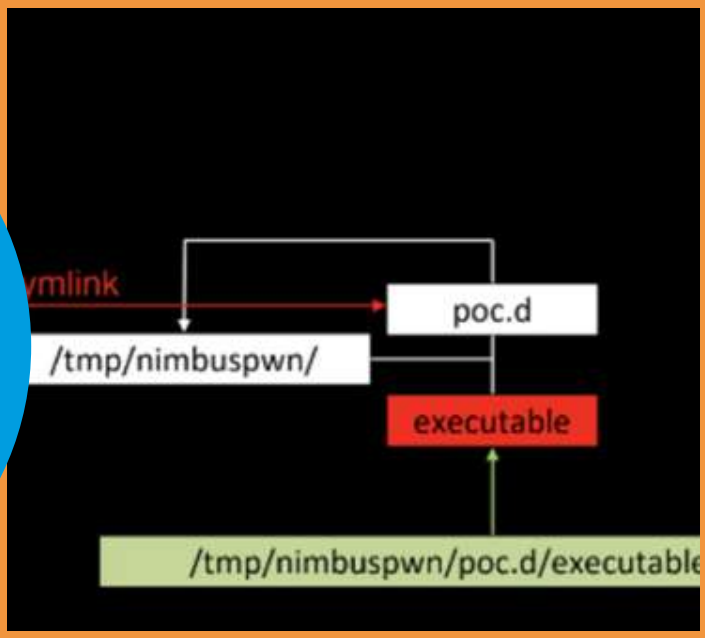
La compañía espera revelar más detalles sobre la falla una vez que la mayoría de los usuarios hayan actualizado a la última versión de Chrome. También tenga en cuenta que esta será la tercera vulnerabilidad de día cero que Google corrige desde principios de 2022.

A la fecha se encuentra parchada la vulnerabilidad, es importante actualizar nuestros navegadores con frecuencia.

NIMBUSPWN, UNA VULNERABILIDAD EN NETWORKD-DISPATCHER QUE PERMITE EJECUTAR COMANDOS COMO ROOT

26/04/2022

LOS INVESTIGADORES DE SEGURIDAD DE MICROSOFT DIERON A CONOCER LA NOTICIA DE QUE HAN IDENTIFICADO DOS VULNERABILIDADESEN EL SERVICIO NETWORKD-DISPATCHER CON NOMBRE EN CÓDIGO NIMBUSPWN



Fuente: Team, M. D. R. (2022, 26 abril). Microsoft finds new elevation of privilege Linux vulnerability, Nimbuspwn. Microsoft Security Blog. https://www.microsoft.com/security/blog/2022/04/26/microsoft-findsnew-elevation-of-privilege-linux-vulnerability-nimbuspwn/

PERMITE A UN USUARIO SIN PRIVILEGIOS EJECUTAR COMANDOS COMO ROOT

Los investigadores de seguridad de Microsoft dieron a conocer la noticia de que han identificado dos vulnerabilidades (CVE-2022-29799, CVE-2022-29800) en el servicio networkd-dispatcher con nombre en código Nimbuspwn el cual permite a un usuario sin privilegios ejecutar comandos como root, permitiendo a los atacantes el de payloads o scripts, que pueden contener ransomware o algpun tipo de malware.
Networkd-dispatcher es utilizado por muchas distribuciones de Linux, incluido Ubuntu, que utiliza el proceso de fondo systemd-networkd para configurar los ajustes de red y realiza funciones similares a NetworkManager-dispatcher, es decir, se ocupa de la ejecución de scripts cuando cambia el estado de la conexión de red, por ejemplo, se utiliza para iniciar una VPN después de establecer la conexión de red principal.

El proceso en segundo plano asociado con networkd-dispatcher se ejecuta como root y escucha eventos a través del D-Bus. El servicio systemd-networkd envía información sobre eventos relacionados con el cambio de estado de las conexiones de red.

Systemd-networkd está diseñado para ejecutar solo secuencias de comandos del controlador del sistema ubicadas en el directorio /etc/networkd-dispatcher y no reemplazable por el usuario, pero debido a una vulnerabilidad (CVE-2022-29799) era posible que el código de manejo de la ruta del archivo se apagara del directorio base de los límites y ejecutar scripts arbitrarios.

QRISHING, AUMENTO DEBIDO A LA PANDEMIA Y LA POPULARIZACIÓN DE LOS QR

18/01/2022

EL USUARIO ACCEDA A LA WEB FRAUDULENTA, Y SE REALIZA ESCANEANDO LA URL CONTENIDA EN UN CÓDIGO QR.

Expansión. (2022, 18 enero). Qrishing: Así usan los códigos QR para robarte dinero y datos personales. Expansión. https://expansion.mx/tecnologia/2022/01/18/qrishing-codigos-qrrobar-dinero-datos

PODRÍAMOS DEFINIR EL QRISHING COMO UNA VARIACIÓN DEL "PHISHING"

Cuando la posible víctima accede a un sitio web fraudulenta cuyo objetivo es que introduzca sus credenciales de usuario u otra información sensible que queda en manos del ciberdelincuente. La técnica usada en el QRishing consiste en que el usuario acceda a la web fraudulenta, y se realiza escaneando la URL contenida en un código QR.

Un elemento de riesgo que podría añadir es que, según la aplicación QR que se emplee y su configuración, ésta puede abrir directamente el enlace sin que el usuario tenga ocasión de verlo primero y comprobar si coincide con el dominio legítimo de la web en cuestión.

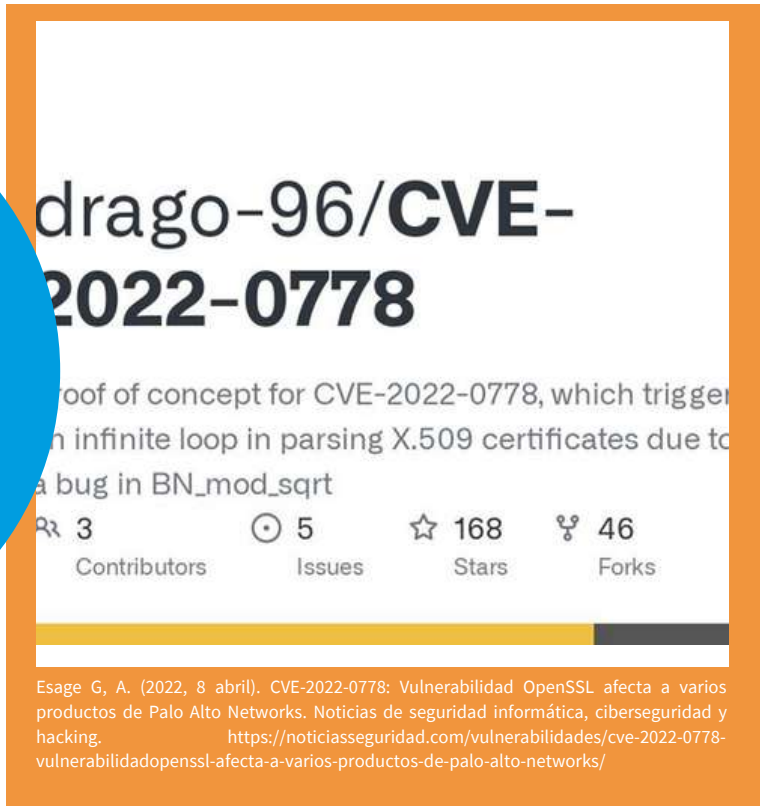
¿Cómo podemos protegernos de las estafas con código QR?

- Desconfiar de los correos que llegan a la bandeja de spam.
- Verificar que el sitio al que te enlazan es el sitio oficial de donde quieres acceder
- Verifica que cuentan con el protocolo HTTPS.
- Desconfiar de códigos QR cuya procedencia no esté verificada.
- Una opción extra implicaría descargar aplicaciones como QR Scanner Kaspersky que busca contenidos maliciosos en los códigos de este tipo.

ALERTA POR VULNERABILIDAD TIPO ALTA (CVE-2022-0778)

02/04/2022

OPENSSL LANZARON UN CONJUNTO DE ACTUALIZACIONES PARA ABORDAR UNA VULNERABILIDAD DE ALTA SEVERIDAD



Esage G, A. (2022, 8 abril). CVE-2022-0778: Vulnerabilidad OpenSSL afecta a varios productos de Palo Alto Networks. Noticias de seguridad informática, ciberseguridad y hacking. https://noticiasseguridad.com/vulnerabilidades/cve-2022-0778-vulnerabilidadopenssl-afecta-a-varios-productos-de-palo-alto-networks/

UN ERROR OPENSSL EN PALO ALTO NETWORK FIREWALLS

Hace un par de semanas, los mantenedores de la biblioteca OpenSSL lanzaron un conjunto de actualizaciones para abordar una vulnerabilidad de alta severidad en la función BN_mod_sqrt() para el análisis de certificados. Identificada como CVE-2022-0778, la vulnerabilidad fue descubierta por expertos de Google Project Zero, quienes mencionan que su explotación exitosa permitiría el despliegue de ataques de denegación de servicio (DoS).

La mencionada vulnerabilidad afecta las versiones 1.0.2, 1.1.1 y 3.0 de OpenSSL.

NOTICIAS NACIONALES

SAQUEO DE DATOS EN EL SAT “POR AÑOS”

25/04/2022

AL MENOS 40 MIL PERSONAS ACCEDIERON A DATOS E INFRAESTRUCTURA DE RED DEL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA (SAT).

Fuente: Saqueo de datos en el SAT. (2022, 25 abril). El Clarinete. https://www.elclarinete.com.mx/saqueo-dedatos-en-el-sat/

“35 MIL PUERTOS DE USUARIOS QUE TENÍAN ACCESO A TODA LA INFORMACIÓN DEL SAT”

Según datos de la funcionaria Raquel Buenrostro, durante los primeros tres meses que a la fecha de inicio de su cargo encontraron tres cables que salían de los servidores del SAT (…) “salían de aquí a instituciones”

Explicó que en ese momento se encontraron “35 mil puertos de usuarios que tenían acceso a toda la información del SAT” todos en estado anónimo, bajo seudónimos como: “patito1, patito2, sinvergüenza2”. La mayor parte de las tecnologías del organismo se contrataban con proveedores.

Los datos también estuvieron expuestos a 250 sitios en entidades federativas múltiples, al Instituto Mexicano del Seguro Social, al Instituto del Fondo Nacional de la Vivienda para los Trabajadores y de vez en cuando, “hace muchos años”, también al Instituto Nacional Electoral; así que la fuga de información tiene varios frentes

Agregando que no se encuentra mucha información distribuida en la red debido a la escala de la vulneración de datos, se desconoce la cantidad de información comprometida.

La solución a corto plazo es desconectar a los usuarios que no deben tener acceso a la red, se analizan los convenios de intercambio de información y se fortalecen las áreas de tecnologías del SAT.

ES MÉXICO PAÍS DE LATINOAMÉRICA CON MÁS CIBERATAQUES

28/04/2022

LOS ATAQUES CIBERNÉTICOS PROVOCAN HASTA CINCO BILLONES DE DÓLARES EN PÉRDIDAS PARA LOS PAÍSES DE LATINOAMÉRICA, EN DÓNDE MÉXICO OCUPA EL PRIMER LUGAR EN CIBERATAQUES

Es México país de Latinoamérica con más ciberataques. (2022, 28 abril). Esquina 32. https://esquina32.info/2022/04/es-mexico-pais-de-latinoamerica-con-mas-ciberataques/

UNA DE LAS PRÁCTICAS MÁS COMUNES DE ROBO DE DATOS ES A TRAVÉS DEL “PHISHING” Y SECUESTRO DE INFORMACIÓN,

Los ataques cibernéticos provocan hasta cinco billones de dólares en pérdidas para los países de Latinoamérica, en dónde México ocupa el primer lugar en ciberataques

Una de las prácticas más comunes de robo de datos es a través del “phishing” y secuestro de información, por ello se debe comenzar con una educación relacionada a la protección de los datos personales cuando se navegue por la web.

Con la tendencia al incremento exponencial de ciberataques en el mundo y en México, hay que permanecer alertas, pero, sobre todo, informarse sobre cómo actuar para prevenir o reaccionar ante uno de ellos.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: ABRIL 2022

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-27342	04/22/2022	SQL inyection a via Link-Admin	CVSS v3.1: [crítico]	NVD - CVE-2022-27342 (nist.gov)

Descripción: Link-Admin v0.0.1 was discovered to contain a SQL injection vulnerability via DictRest.ResponseResult().

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-27341	04/22/2022	Fallas de seguridad en productos SQL	CVSS v3.1:9.8 [crítico]	NVD - CVE-2022-27341 (nist.gov)

Descripción: JFinalCMS v2.0 was discovered to contain a SQL injection vulnerability via the Article Management function.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-26674	04/22/2022	Acceso remoto sin autenticación encontrado en productos ASUS RT-AX88U	CVSS v3.1:9.8 [crítico]	NVD - CVE-2022-26674 (nist.gov)

Descripción: ASUS RT-AX88U has a Format String vulnerability, which allows an unauthenticated remote attacker to write to arbitrary memory address and perform remote arbitrary code execution, arbitrary system operation or disrupt service.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-28439	04/21/2022	Baby Care System	CVSS v3.1:9.8 [crítico]	NVD - CVE-2022-28439 (nist.gov)

Descripción: Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&&action=delete&userid=4.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-28438	04/21/2022		CVSS v3.1:9.8 [crítico]	NVD - CVE-2022-28438 (nist.gov)

Descripción: Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&action=type&userrole=User&userid=.

TABLA DE VULNERABILIDADES RELEVANTES: ABRIL 2022

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-28437	04/21/2022		CVSS v3.1:9.8 [crítico]	NVD - CVE-2022-28437 (nist.gov)

Descripción: Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&action=type&userrole=Admin&userid=3.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-28436	04/21/2022		CVSS v3.1: 9.8 [crítico]	NVD - CVE-2022-28436 (nist.gov)

Descripción: Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&action=display&value=Hide&userid=.

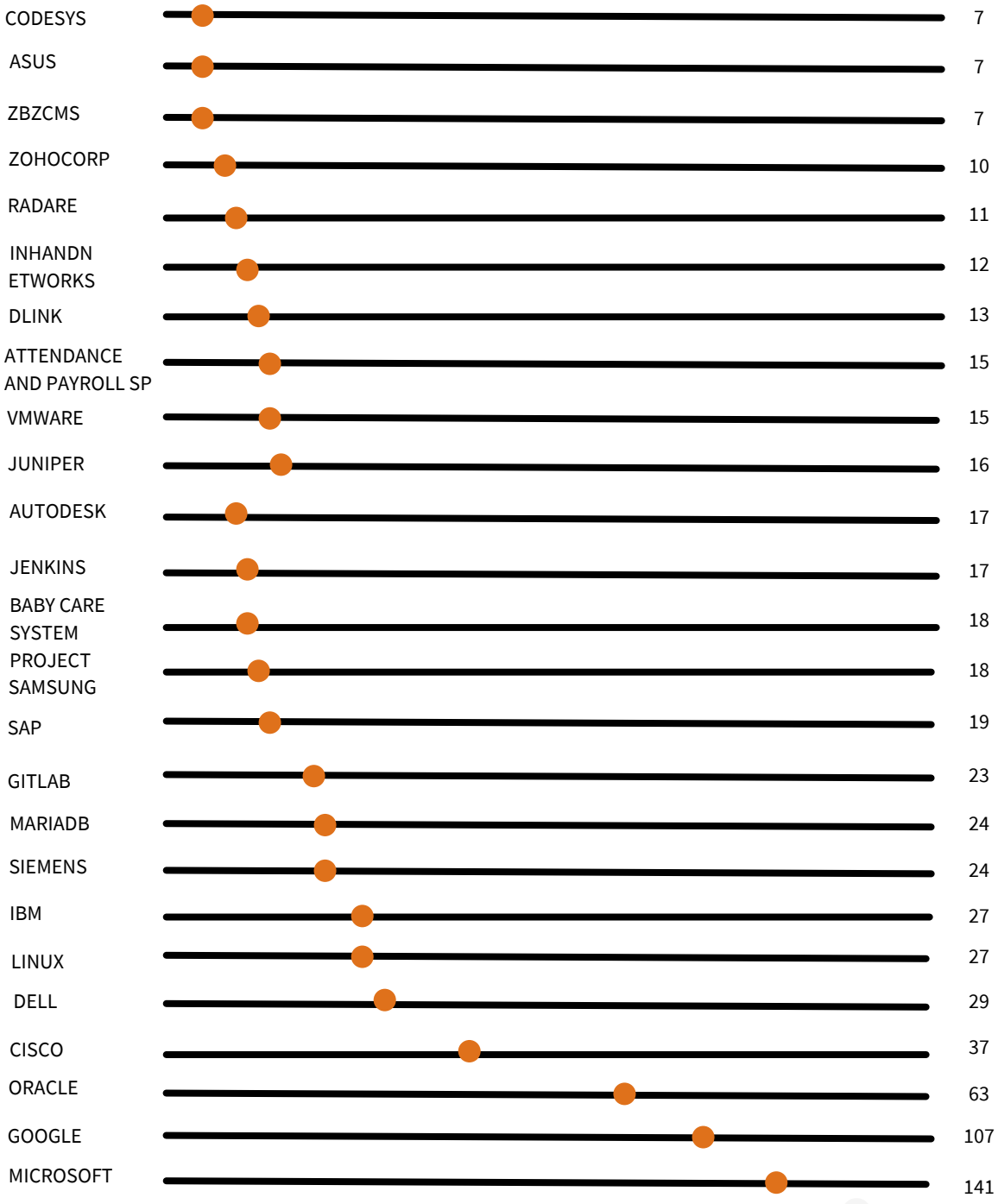
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-28435	04/21/2022		CVSS v3.1:9.8 [crítico]	https://nvd.nist.gov/vuln/detail/CVE-2022-28435

Descripción: Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/siteoptions.php&action=displaygoal&value=1&roleid=1.

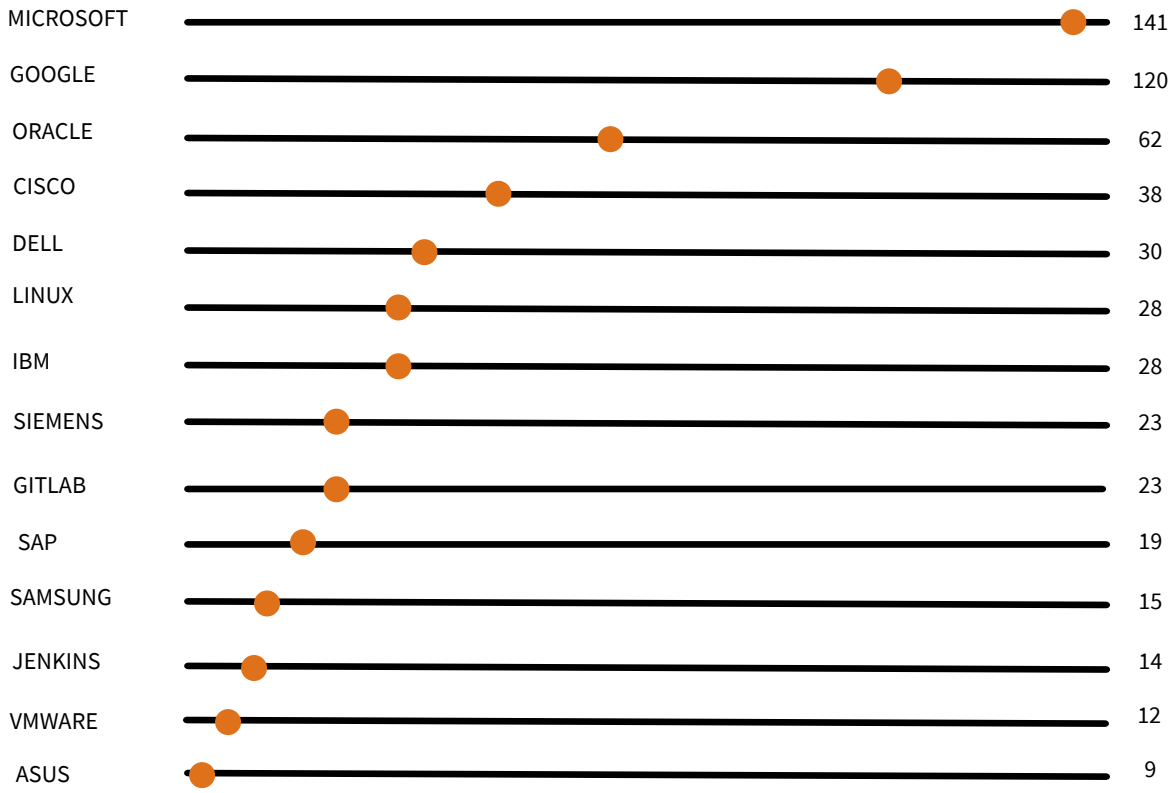
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-28434	04/21/2022		CVSS v3.1:9.8 [crítico]	https://nvd.nist.gov/vuln/detail/CVE-2022-28434

Descripción: Baby Care System v1.0 was discovered to contain a SQL injection vulnerability via /admin/uesrs.php&action=display&value=Show&userid=.

FABRICANTES Y SUS VULNERABILIDADES RELEVANTES: MARZO DE 2022



EMPRESAS MULTINACIONALES Y SUS VULNERABILIDADES: MARZO DE 2022



CULTURA DE CIBERSEGURIDAD

ATT&CK DE MITRE

¿QUÉ ES ATT&CK DE MITRE?

MITRE presentó ATT&CK **(tácticas, técnicas y conocimiento común de adversarios)** en el 2013 como una forma de describir y clasificar los comportamientos adversarios con base en observaciones reales. **ATT&CK** es una lista estructurada de comportamientos conocidos de atacantes recopilados en tácticas y técnicas, y expresados en varias matrices, así como a través de STIX y TAXII. Debido a que esta lista es una representación bastante integral de los comportamientos que emplean los atacantes al comprometer las redes, es útil para una variedad de mediciones ofensivas y defensivas, representaciones y otros mecanismos. Entre las matrices, además de la relacionada con Sistemas de Control Industrial, pueden consultarse otras que también aportan información de interés:

- **PRE-ATT&CK –** Matriz que recopila las tácticas y técnicas detectadas en algunos ataques y que guardan estrecha relación con las dos primeras fases (reconocimiento y preparación) de la taxonomía de ataque propuesta por Loocked Martin (Cyber Kill Chain). Podría decirse que en esta matriz se recopilan los trabajos previos al ataque.

- **Enterprise –** Relacionada con ataques en entornos corporativos. Dado que los entornos corporativos evolucionan tanto como la tecnología que se despliega dentro de los mismos, se han creado diferentes submatrices dependiendo del sistema operativo (Windows, macOS y Linux) y algunas tecnologías como la Cloud (AWS, GCP, Azure, Office 365, Azure AD, SaaS).

- **Mobile –** MITRE ha incorporado dentro de sus matrices dos específicas para tratar dispositivos móviles, una relacionada con el acceso a dispositivos, y otra para efectos originados en la red que pueden ser utilizados por adversarios sin acceso a dispositivos. Se han definido para sistemas iOS y Android.

DETALLES DE ATT&CK: TÁCTICAS Y TÉCNICAS

Cuando se observa **ATT&CK** en forma de matriz, los títulos de las columnas en la parte superior son **tácticas** y, básicamente, categorías de técnicas. Las tácticas corresponden a **qué** intentan lograr los atacantes, mientras que las técnicas individuales corresponden a **cómo** logran esos pasos u objetivos.

ATT&CK DE MITRE

LAS DIFERENCIAS ENTRE PRE-ATT&CK Y ATT&CK ENTERPRISE

PRE-ATT&CK y ATT&CK Enterprise se combinan para formar la lista completa de tácticas que en términos generales se alinean con la cadena de ataque informático. **PRE-ATT&CK** se alinea principalmente con las primeras tres fases de la cadena de ataque: reconocimiento, armamentización y entrega. **ATT&CK** Enterprise se alinea de buena manera con las cuatro fases finales de la cadena de ataque: explotación, instalación, comando & control, y acciones en objetivos.

Tácticas de PRE-ATT&CK	Tácticas de ATT&CK Enterprise
Definición de prioridad	Acceso inicial
Selección de destino	Ejecución
Recopilación de información	Persistencia
Identificación de debilidades	Escalamiento de privilegios
Seguridad de las operaciones del adversario	Evasión de defensa
Establecimiento y mantenimiento de la infraestructura	Acceso a credenciales
Desarrollo personal	Descubrimiento
Capacidades de desarrollo	Movimiento lateral
Capacidades de prueba	Recopilación
Capacidades de montaje	Exfiltración
	Comando y control

¿PARA QUÉ SIRVE ATT&CK?

ATT&CK es valioso en una variedad de situaciones diarias. Cualquier actividad defensiva que haga referencia a los atacantes y a sus comportamientos puede beneficiarse de la aplicación de la taxonomía de **ATT&CK.** Además de ofrecer un léxico común para los defensores informáticos, **ATT&CK** también proporciona una base para las pruebas de penetración y la creación de equipos rojos. Esto brinda un lenguaje común para los defensores y los equipos rojos cuando se refieren a comportamientos adversarios.

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://blog.elhacker.net/2022/04/el-fbi-hace-oficial-el-cierre-de-RaidForums-y-detieneadministrador-omnipotent-portugues-21-edad.html
- https://hackwise.mx/esta-grave-vulnerabilidad-de-java-permite-falsificar-certificados-y-firmas-tls/
- https://es.postsus.com/technology/208334.html
- https://www.microsoft.com/security/blog/2022/04/26/microsoft-findsnew-elevation-of-privilege-linux-vulnerability-nimbuspwn/
- https://expansion.mx/tecnologia/2022/01/18/qrishing-codigos-qrrobar-dinero-datos
- https://noticiasseguridad.com/vulnerabilidades/cve-2022-0778-vulnerabilidadopenssl-afecta-a-varios-productos-de-palo-alto-networks/
- https://www.elclarinete.com.mx/saqueo-dedatos-en-el-sat/
- https://www.anomali.com/es/resources/what-mitre-attck-is-and-how-itis-useful#:~:text=ATT%26CK%20puede%20ser%20%C3%BAtil%20para,que%2 0se%20sabe%20que%20utilizan.
- https://www.incibe-cert.es/blog/matriz-mitre-tacticas-y-tecnicasentornos-industriales https://attack.mitre.org/#

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