BOLETÍN DE CIBERSEGURIDAD

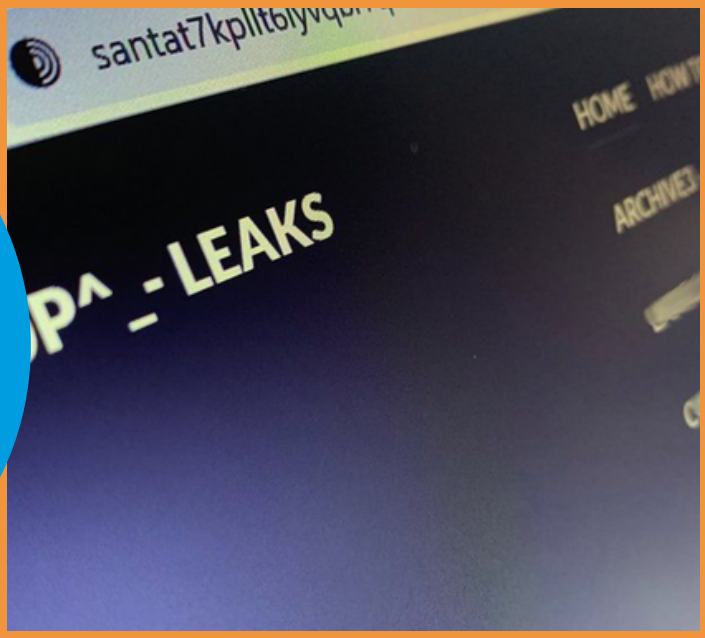
JUNIO 2023

ÍNDICE

NOTICIAS INTERNACIONALES

ATAQUE MOVEIT: EL GRUPO DE RANSOMWARE CLOP APROVECHA UNA VULNERABILIDAD

LOS PRIMEROS RUMORES SOBRE EL ERROR DE MOVEIT COMENZARON HACE POCO MÁS DE UNA SEMANA, CUANDO EL PROVEEDOR DE SERVICIOS DE NÓMINA ZELLIS CONFIRMÓ QUE ÉL ERA EL ORIGEN DE LA INFRACCIÓN, QUE A SU VEZ COMPROMETIÓ A VARIOS DE SUS CLIENTES.



Ikeda, S. (2023, 20 junio). MOVEit Cyber Attack Has Many More Victims Than Previously Thought; Attackers Experimented With Vulnerabili . . . CPO Magazine. https://www.cpomagazine.com/cyber-security/moveit-cyber-attack-has-many-more-victims-than-previously-thought-attackers-experimented-with-vulnerability-since-2021/
Tidy, B. J. (2023, 20 junio). MOVEit hack: Gang claims not to have BBC, BA and Boots data. BBC News. https://www.bbc.com/news/technology-65965453

En ese momento, se especuló que la vulnerabilidad se utilizó para infiltrarse en múltiples organizaciones.

Esto fue confirmado por la pandilla de ransomware Cl0p, que publicó una lista de víctimas que ha recopilado desde mayo. El llamado "primer grupo objetivo" incluye agencias gubernamentales federales y estatales, los principales bancos y firmas de inversión, y universidades. Muchas organizaciones están trabajando actualmente para evaluar los daños, pero ya se han descubierto algunas infracciones catastróficas, incluida la aparente exposición de casi todas las licencias de conducir y números de seguro social registrados en Luisiana.

El desarrollador de MOVEit, Progress Software, reveló la vulnerabilidad el último día de mayo e instó a todos los clientes a actualizar su software rápidamente. El primer indicio de explotar esta vulnerabilidad se produjo a principios de junio, cuando el proveedor de nóminas británico Zellis confirmó que había sido atacado por un ciberataque que robó datos de varios clientes, incluidos British Airways, BBC y Aer Lingus.). Pero muchas otras empresas usan MOVEit y los atacantes explotaron activamente la vulnerabilidad antes de que se hiciera pública.

INTERRUPCIONES DE MICROSOFT AZURE Y OUTLOOK CAUSADAS POR UN ATAQUE DDOS

MICROSOFT ALEGA QUE STORM-1359 INICIÓ VARIOS ATAQUES DDOS DE CAPA 7, INCLUIDO UN ATAQUE DE INUNDACIÓN HTTP(S), QUE REQUIERE UNA GRAN CANTIDAD DE PROTOCOLOS DE ENLACE SSL/TLS Y SOLICITUDES HTTP (S), LO QUE LLEVA AL USO DE LA CPU Y AL AGOTAMIENTO DE LA MEMORIA.

MSN. (s. f.). https://www.msn.com/en-us/news/technology/microsoft-azure-and-outlook-outages-were-caused-by-ddos-attacks/ar-AA1cKjin

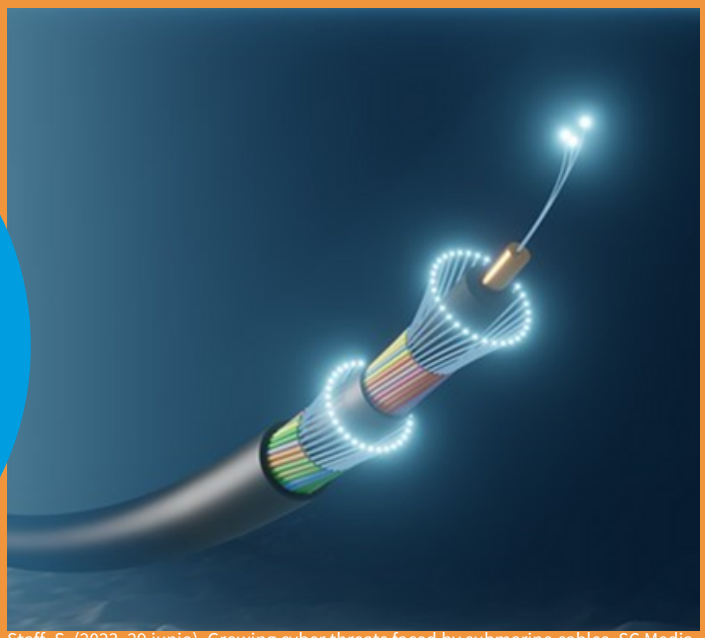
. Se cree que millones de solicitudes se hicieron al mismo tiempo en este caso.
El grupo empleó técnicas como la evasión de caché, que obliga a la capa frontend a redirigir las solicitudes al origen en lugar de reutilizar el contenido almacenado en caché, y slowloris, otra técnica que obliga a un servidor web a mantener la conexión al no reconocer las notificaciones de descarga cuando se establece la conexión.

La declaración de Microsoft sugiere que es probable que los ataques se basen en el acceso a múltiples servidores privados virtuales (VPS) y otra infraestructura de nube de alquiler, así como proxies abiertos y herramientas DDoS. A pesar de la interrupción de los servicios durante varios días a principios de junio, Microsoft afirma que no hay indicios de que se haya accedido o comprometido los datos de los clientes. "Es solo cuestión de conseguir algo".

En su sitio web, la compañía ha brindado a los clientes un conjunto de pasos que pueden ayudarlos a minimizar el impacto de los ataques DDoS de Capa 7 en el futuro.

CRECIENTES CIBERAMENAZAS PARA LOS CABLES SUBMARINOS

SEGÚN SECURITYWEEK, HA HABIDO UN AUMENTO EN LAS AMENAZAS DE SEGURIDAD CIBERNÉTICA CONTRA CABLES SUBMARINOS, SIENDO LAS OPERACIONES DE AMENAZAS PATROCINADAS POR EL ESTADO EL PROBLEMA MÁS IMPORTANTE DEBIDO A LAS TENSIONES GEOPOLÍTICAS ENTRE EE. UU. Y CHINA



Staff, S. (2023, 29 junio). Growing cyber threats faced by submarine cables. SC Media. https://www.scmagazine.com/brief/incident-response/growing-cyber-threats-faced-by-submarine-cables
Coker, J. (2023, 27 junio). Submarine Cables at Growing Risk of Cyber-Attacks. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/submarine-cables-risk-cyber-attacks/

Un informe de Recorded Future ha revelado que el control digital del flujo por parte de China le ha permitido utilizar nuevos métodos de recopilación de información, lo que lo convierte en una amenaza importante para los cables submarinos, mientras que la incapacidad de Rusia para gastar sus recursos en cortar cables submarinos plantea riesgos draconianos.

Además de atacar las estaciones de aterrizaje, las operaciones cibernéticas respaldadas por el estado también podrían usar las crecientes capacidades de los sistemas de administración de redes remotas (RNS) para facilitar los ataques. Es probable que todo el ecosistema de cables submarinos, incluida su infraestructura, hardware y software, sea el objetivo de los agentes estatales que buscan información para obtener una ventaja en el espionaje. Eso lo resume. Es muy probable que Rusia intensifique sus esfuerzos para mapear cables submarinos, incluidas operaciones tanto abiertas como encubiertas, y se involucre en sabotajes dirigidos en tierra y bajo el agua.

200,000 SITIOS DE WORDPRESS ESTÁN BAJO ATAQUE USANDO VULNERABILIDADES CON UN PLUGIN "ULTIMATE MEMBER"

ESTE COMPLEMENTO ESTÁ DISEÑADO PARA QUE SEA MÁS FÁCIL PARA LOS USUARIOS REGISTRARSE E INICIAR SESIÓN EN SU SITIO WEB.

Arghire, I. (2023). 200,000 WordPress Sites Exposed to Attacks Exploiting Flaw in 'Ultimate Member' Plugin. SecurityWeek. https://www.securityweek.com/200000-wordpress-sites-exposed-to-attacks-exploiting-flaw-in-ultimate-member-plugin/?web_view=true

Permite a los propietarios de sitios agregar perfiles de usuario, definir roles, crear campos de formulario personalizados y directorios de miembros, y más.

Una vulnerabilidad de Ultimate Member identificada recientemente, rastreada como CVE-2023-3460 (puntaje CVSS de 9.8), permite a los atacantes agregar nuevas cuentas de usuario al grupo de administradores.

Algunos usuarios del complemento observaron e informaron sobre la creación de cuentas fraudulentas esta semana, y los ataques parecen haber estado en curso desde al menos principios de junio. Según la empresa de seguridad de WordPress, WPScan, el problema se debe a un conflicto entre la lógica de la lista de bloqueo del complemento y la forma en que WordPress maneja las metaclaves.

Ultimate Member utiliza listas negras para almacenar metaclaves que los usuarios no deben manipular y verifica estas listas cada vez que un usuario intenta registrar estas claves durante la creación de la cuenta. WPScan explicó que debido a las diferencias en la funcionalidad entre el complemento y WordPress, un atacante podría engañar al complemento para que actualice las metaclaves, como las que almacenan las funciones y habilidades de los usuarios. La empresa proporciona indicadores de compromiso (IoC) relacionados con los ataques observados.

Se recomienda a los propietarios del sitio que deshabiliten Ultimate Member para evitar la explotación de la vulnerabilidad. También debe revisar todos los roles de administrador en su sitio web para identificar cuentas falsas.

BYTEHIDE GANA LA COMPETENCIA DE STARTUPS EN LA NUBE POR UN PROYECTO DE CIBERSEGURIDAD EN LA NUBE

EL RECIENTE STARTUP TECHDAY REUNIÓ A UN GRAN NÚMERO DE EXPERTOS DEL ECOSISTEMA DE STARTUPS DE MADRID, ENTRE LOS QUE SE ENCONTRABAN FUNDADORES, CEOS, RESPONSABLES TECNOLÓGICOS Y EXPERTOS EN CLOUD COMPUTING

SLU, T. T. (s. f.). ByteHide gana la Startup Cloud Competition con su proyecto de Ciberseguridad en la nube. Telefónica Tech. https://telefonicatech.com/actualidad/bytehide-gana-la-startup-cloud-competition-proyecto-ciberseguridad-en-cloud

Uno de los aspectos más destacados es la empresa emergente Cloud Competition, un concurso organizado por Telefónica Tech y Altostratus, parte de Wayra, destinado a premiar los proyectos tecnológicos más innovadores en el espacio de la nube.

El startup ganador fue ByteHide, que se centra en la ciberseguridad en la nube. El fundador y CEO de ByteHide, Juan Alberto España, recogió el premio en una ceremonia a la que asistieron compañeros de la División AltStratus de Telefónica Technology, Weira y Telefónica.

ByteHide es proporcionado por Wayra y Altostratus, parte de Telefónica Tech. Como recompensa, obtienes acceso al espacio físico en las oficinas de Wayra y ventajas como el análisis priorizado de posibles inversiones. Además, Altostratus, parte de Telefónica Tech, proporcionará soporte técnico y servicios profesionales por valor de 10.000 € para mejorar su desarrollo y habilidades técnicas.
Impulsado por Altostratus Part de Telefónica Tech en asociación con Google Cloud, Startup TechDay fue un foro para compartir conocimientos y establecer contactos entre startups, aceleradoras, fondos de inversión y empresas patrocinadoras.

El evento contó con presentaciones de expertos en tecnología y entorno cloud como Jorge Nogales, Customer Engineering Manager de Google Cloud. Jose Luis Serrada, CTO de Altostratus, parte de Telefónica Tech. Además, a lo largo de la jornada también se trataron temas como cómo acelerar los startups y los retos de invertir en proyectos deep tech con la participación de firmas de capital riesgo y corporativo como Adara Ventures, Elewit, Swanlaab Venture Factory y Kibo Ventures.

GOOD TECH TIMES: OPTIMIZACIÓN DEL GASTO EN LA NUBE CON AWS PARA ACENS

LAS REUNIONES EN LÍNEA SOBRE METODOLOGÍAS FINOPS COMBINADAS CON MARCOS DE BUENAS PRÁCTICAS BIEN DISEÑADOS BRINDAN CONTEXTO PARA ADMINISTRAR COSTOS Y ASIGNARLOS A DIFERENTES EQUIPOS

SLU, T. T. (s. f.-b). Good Tech Times: Optimiza tu gasto en La Nube con AWS by acens. Telefónica Tech. https://telefonicatech.com/actualidad/1600-cest-good-tech-times-optimiza-tu-gasto-en-la-nube-con-aws-by-acens

Esta visibilidad permite a las organizaciones tomar decisiones basadas en datos sobre cómo optimizar el uso de la nube y maximizar el retorno de la inversión. El marco de buena arquitectura, por otro lado, proporciona un conjunto de mejores prácticas para diseñar y operar sistemas confiables, seguros, eficientes y rentables en la nube. Al seguir estas pautas, puede optimizar sus esfuerzos en términos de rendimiento, escalabilidad y seguridad mientras minimiza los costos operativos.

Vocero:

- David Salazar - Especialista en ventas de Telefónica Tech Cloud
- Manuel Eusebio de Paz Carmona – AWS Enterprise Architect en Telefónica Tech
- Alejandro Moreno - Parte de Business Development AWS Gran Cuenta Este en acens Telefónica Tech

NOTICIAS NACIONALES

GUARDIA NACIONAL ADVIERTE SOBRE POSIBLE FUGA DE BASE DE DATOS BANCARIA

EL CENTRO DE RESPUESTA A INCIDENTES (CERT-MX) DE LA GUARDIA NACIONAL DE MÉXICO (GN) SOLICITÓ A LAS INSTITUCIONES DEL SISTEMA FINANCIERO ASEGURAR SUS BASES DE DATOS

El Economista. (s. f.). ciberseguridad, Noticias sobre ciberseguridad | El Economista. https://www.eleconomista.com.mx/tags/ciberseguridad

Documentos investigados por los medios muestran que la posible filtración fue descubierta en un foro conocido como Dark Forum, un espacio para discutir juegos, tecnología y otros temas relacionados con el crimen.

Al respecto, CERT-MX afirma tener datos de dos instituciones financieras que contienen más de 9 millones de registros de información personal y financiera como nombres, direcciones, teléfonos, números de clientes, números de clientes, etc. Encontré una publicación de usuarios reclamados 'wht' y 'ar3s'. Detalles del producto, principalmente relacionados con tarjetas de crédito.
Un documento del CERT-MX fechado el 14 de junio establece: "El usuario 'wht' hizo dos revelaciones en junio de dos bases de datos supuestamente propiedad de dos instituciones financieras... al menos una ya ha sido revelada en un foro similar en los últimos años".

Esta alerta ha sido calificada como "muy importante" e insta a los miembros del sistema financiero a tomar medidas para prevenir incidentes relacionados con este evento. Entre las acciones recomendadas, destaca verificar si los datos filtrados corresponden a su organización o usuarios. Notifique a los afectados, brinde orientación sobre cómo fortalecer las medidas de seguridad para protegerse contra posibles consecuencias adversas en caso de que una infracción afecte a los clientes.

MÉXICO AVANZA CERCA DE UN CARIÑO DE CIBERSEGURIDAD

LA ORGANIZACIÓN INTERNACIONAL DE HACKERS Y EXPERTOS EN CIBERSEGURIDAD (OIHEC), ENCABEZADA Y FUNDADA POR HÉCTOR LÓPEZ, FUE ÚNICO DE LA COMPAÑÍA CONSULTADOS DURANTE EL PRIMER TROTE DE CIBERSEGURIDAD LEGISLATIVA Y DE POLÍTICA PÚBLICA

Ortega, R. (2023). México avanza hacia una ley de ciberseguridad. eSemanal - Noticias del Canal. https://esemanal.mx/2023/06/mexico-avanza-hacia-una-ley-de-ciberseguridad/

En exclusiva para eSemanal, el cursado manifestó su enardecimiento por la circunstancia positiva de la ciberseguridad en México y señaló la desestimación potencia en organismos de gestión y que por punto pueden cuerpo hackeados preciso a la pobreza de un borrador tipificado y estandarizado en cuanto a el establecimiento de programa en los equipos, proponiendo la génesis de un cúmulo privada del gestión para centralizar los servidores y los accesos.

En la trote de ciberseguridad igualmente se dieron referencia otras organizaciones como R3D, que han circunstancia siguiendo de verja las aristas y el contexto del progreso legislativo, planteando la gravedad de estimar nunca romanza a las personas, suerte igualmente a las acciones en la regulación de ciberseguridad en México, haciendo fuerza en la apresuramiento de adecuar las derecho al contexto nacional, considerando las particularidades del distrito en términos de cuentas bancarias, fraudes comunes, ciberataques frecuentes, tributo humanos, autogobierno de aspecto y usufructo de datos privados.

Es elevado balizar que estos foros buscan, menguar y extirpar las eventuales “lagunas” legales que podrían devenir de la amistad proposición por el Diputado Javier López Casarín, del Partido Verde Ecologista de México (PVEM).

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: JUNIO 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-20895	06/22/2023	The VMware vCenter Server contains a memory	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-25909

Descripción: A malicious actor with network access to vCenter Server may trigger a memory corruption vulnerability which may bypass authentication.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-2982	06/28/2023	The WordPress Social Login and Register	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-21058

Descripción: This is due to insufficient encryption on the user being supplied during a login validated through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they know the email address associated with that user. This was partially patched in version 7.6.4 and fully patched in version 7.6.5.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-29357	06/13/2023	Microsoft SharePoint Server Elevation	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-42498

Descripción: Is an EoP vulnerability in Microsoft SharePoint Server 2019 that was assigned a CVSSv3 score of 9.8 and rated critical. A remote, unauthenticated attacker can exploit the vulnerability by sending a spoofed JWT authentication token to a vulnerable server giving them the privileges of an authenticated user on the target.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-23482	06/07/2023	IBM Sterling Partner Engagement	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-20532

Descripción: By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 245891.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-32387	06/23/2023	A use-after-free issue was addressed	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-32387

TABLA DE VULNERABILIDADES RELEVANTES: JUNIO 2023

Descripción: A remote attacker may be able to cause unexpected app termination or arbitrary code execution

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-32216	6/19/2023	Memory safety bugs present in Firefox 112.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-32216

Descripción: Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 113.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-48472	06/16/2023	A Huawei printer has a system command	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-484772

Descripción: Successful exploitation could lead to remote code execution. Affected product versions include:BiSheng-WNM versions OTA-BiSheng-FW-2.0.0.211-beta,BiSheng-WNM FW 3.0.0.325,BiSheng-WNM FW 2.0.0.211.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-27997	06/13/2023	A heap-based buffer overflow vulnerability [CWE-122]	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-27997

Descripción: Version 7.0.11 and below, version 6.4.12 and below, version 6.0.16 and below and FortiProxy version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below, version 1.2 all versions, version 1.1 all versions SSL-VPN may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests.

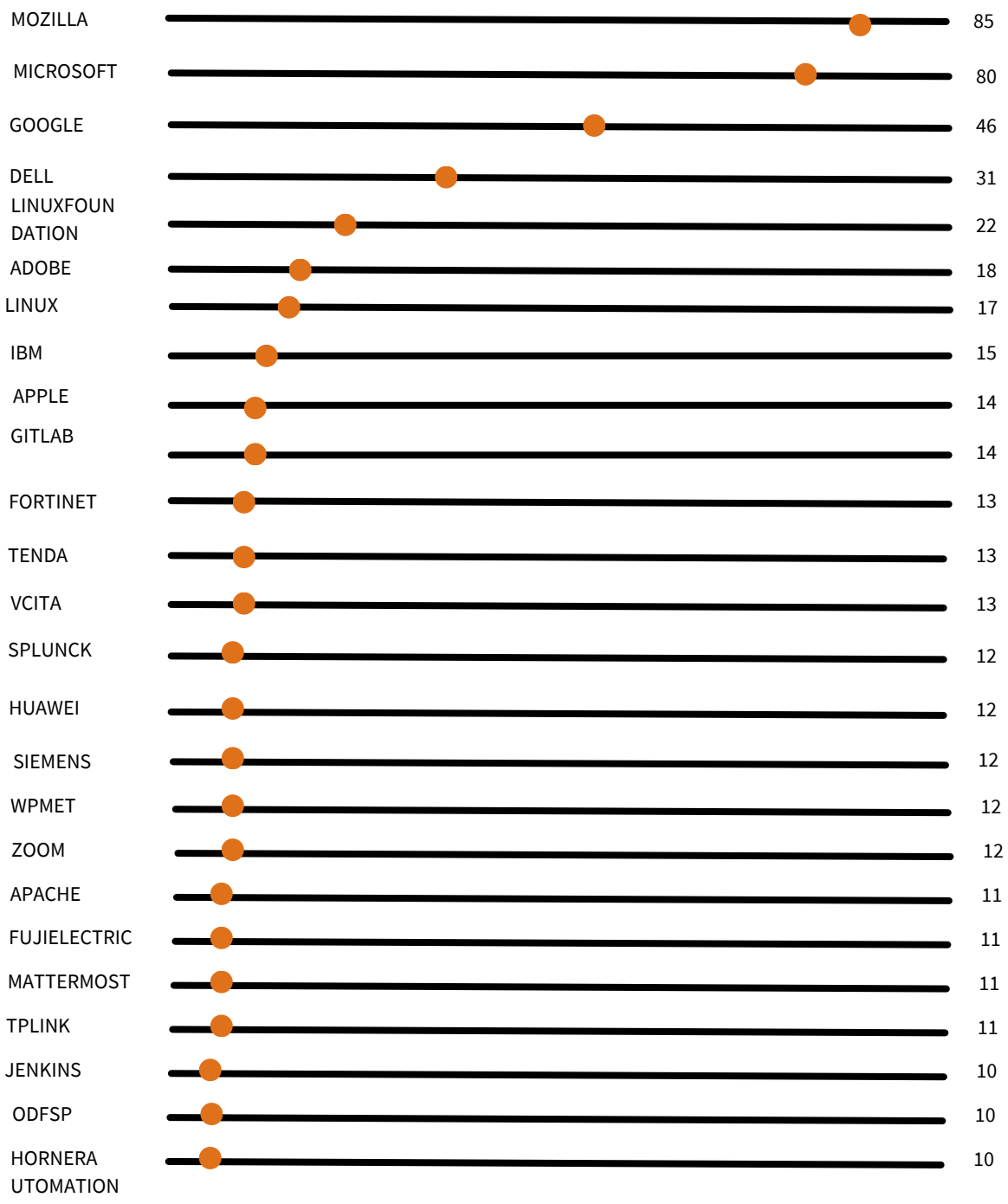
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-32673	06/12/2023	PoC exploit for HP Hardware Diagnostic's EtdSupp	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-32673

Descripción: Certain versions of HP PC Hardware Diagnostics Windows, HP Image Assistant, and HP Thunderbolt Dock G2 Firmware are potentially vulnerable to elevation of privilege.

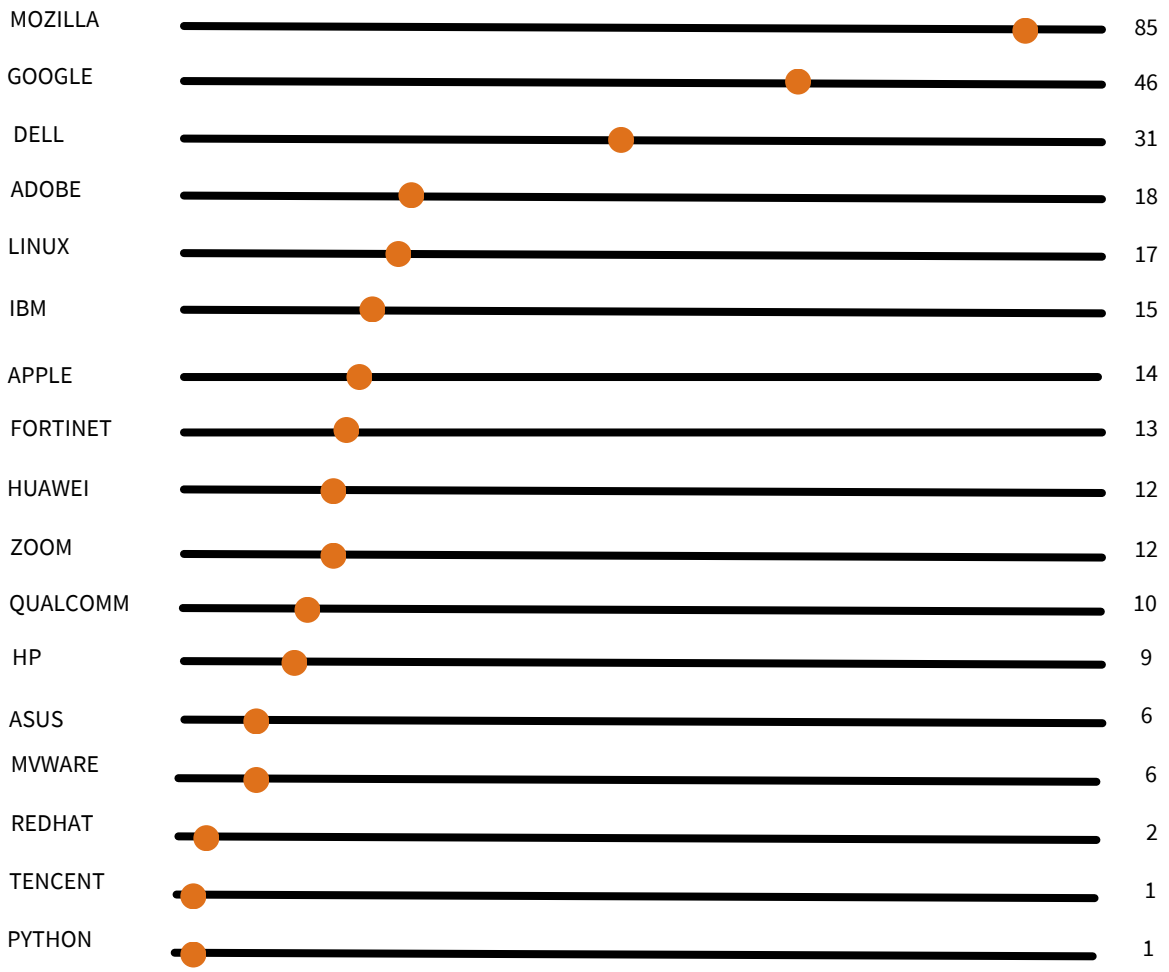
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-34239	06/07/2023	Gradio does not properly restrict the what URLs are proxied.	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-34239

Descripción: Gradio is an open-source Python library that is used to build machine learning and data science. Due to a lack of path filtering Gradio does not properly restrict file access to users. Additionally Gradio does not properly restrict the what URLs are proxied.

FABRICANTES Y SUS VULNERABILIDADES RELEVANTES: JUNIO DE 2023



EMPRESAS MULTINACIONALES Y SUS VULNERABILIDADES: JUNIO DE 2023



CULTURA DE CIBERSEGURIDAD

¿CÓMO SE UTILIZAN LOS ARCHIVOS PDF PARA PROPAGAR MALWARE?

Es muy común que los documentos del paquete de Office, especialmente los archivos de Word y Excel se utilicen para actividades maliciosas a través de macros. Pero ¿son estos los únicos documentos que pueden suponer un riesgo para la seguridad de su equipo? A continuación, explicamos cómo se utilizan los archivos PDF para propagar malware. ¿Qué pasa con los archivos PDF?

Uno de los formatos de almacenamiento de documentos más utilizados en el mundo es PDF. Este formato es muy versátil ya que te permite incorporar diferentes tipos de contenido a tu documento, como, por ejemplo: B. Imágenes, videos, audio, modelos 3D, otros documentos, guiones, etc.

Esta gran versatilidad es muy útil, pero también pueden abusar de ella los ciberdelincuentes que utilizan este tipo de archivos como un medio más para infectar a sus objetivos. Para comprender mejor los archivos PDF maliciosos, primero echemos un vistazo rápido a la estructura básica del formato.

En su versión más simple, consta de cuatro secciones principales:

- Encabezado: ubicado en la parte superior del archivo y contiene solo la versión de la especificación de PDF que se debe usar.
- Cuerpo: Contiene todos los objetos que componen el documento (texto, imágenes, etc.).
- Tabla de referencias cruzadas (xref): contiene la ubicación (dirección dentro del archivo binario) donde se encuentra cada objeto dentro de la estructura interna del archivo. Esto ayuda a evitar tener que buscar en todo el documento para encontrar el objeto de punto.
- Tráiler: contiene dónde comienza la tabla de referencia externa y un indicador de fin de archivo (%EOF).

Un dato interesante de este formato es que requiere leer el archivo de principio a fin debido a su estructura y problemas de rendimiento. De esta forma, puede encontrar la posición de todos los objetos en el archivo comenzando a leer el tráiler, obteniendo la posición de la tabla de referencia externa y conociendo esta posición.

¿CÓMO SUELEN COMPORTARSE LOS PDF MALICIOSOS?

Si bien las dinámicas empleadas por los cibercriminales al momento de diseñar sus PDF maliciosos son muy variadas, existen dos “corrientes” principales:

MEDIANTE EXPLOITS

El PDF malicioso contiene un exploit capaz de aprovechar una vulnerabilidad en el programa con el cual se abre el archivo, comúnmente conocido como lector de PDF. Cabe destacar que no todos los programas presentan las mismas vulnerabilidades e incluso una versión de un programa podría ser vulnerable y otra no. Un ejemplo de esta dinamica es el archivo PDF malicioso analizado en 2018 por investigadores de ESET, donde se descubrio que utilizaba una vulnerabilidad zero-day que afectaba ciertas versiones del popular lector Adobe Reader y que al ser explotada permitía al atacante ejecutar codigo arbitrario en el equipo de la victima de manera remota. En este sentido, estos ataques suelen estár dirigidos únicamente a los usuarios de versiónes específicas de un programa específico. Por esta razón, es aconsejable evitar revelar detalles de los programas utilizados, ya que este tipo de información se puede utilizar en el contexto de ataques dirigidos (más sobre este tema más adelante). a través de un guión.

Para que el ataque sea efectivo, la secuencia de comandos debe ejecutarse automáticamente inmediatamente cuando el usuario abre el PDF. Esto se logra usando comandos específicos de formato como "OpenAction" configurado para abrir scripts.

¿CÓMO SE UTILIZAN LOS ARCHIVOS PDF PARA PROPAGAR MALWARE?

PDF EN ATAQUES CORPORATIVOS

Los archivos PDF están presentes en casi todas las oficinas y actividades comerciales personales a las que servimos. Envío y recepción de folletos de productos, contratos, ofertas de servicios, informes, etc. Los archivos PDF son habituales en entornos corporativos, lo que los convierte en una excelente oportunidad para que los ciberdelincuentes lancen ataques dirigidos.

La complejidad y la dinámica de los ataques que utilizan estos archivos varían según la imaginación del atacante. Los atacantes pueden usar cualquier cosa, desde archivos PDF genéricos enviados en masa a todos los miembros de una organización hasta archivos PDF cuidadosamente elaborados dirigidos a empleados específicos en áreas específicas. . Por ejemplo, un atacante podría crear un documento detallando los requisitos para contratar un servicio, enviarlo a un área de ventas y hacer que el cliente abra el documento para ver si cumple con los requisitos de "cliente potencial".

Muchos archivos PDF maliciosos usan exploits que aprovechan las vulnerabilidades de los lectores de PDF. Estas vulnerabilidades suelen existir solo en versiones específicas del producto, por lo que un exploit podría funcionar en una versión pero no necesariamente en otra. Por lo tanto, antes de lanzar un ataque, los ciberdelincuentes necesitan recopilar información sobre los sistemas y productos utilizados por sus objetivos para aumentar la precisión y eficacia de sus ataques.

Aquí es donde los archivos PDF vuelven a entrar en juego, incluso si son creados legítimamente por la organización atacada. Cuando se genera un documento PDF, generalmente contiene metadatos que brindan información diversa, como el programa que creó el documento PDF y posiblemente el sistema operativo en el que se ejecutaba el software.

Por lo tanto, un atacante podría buscar archivos PDF públicos de la organización que desea atacar e incluso obtener documentos PDF creados para su propio uso haciéndose pasar por clientes. Una vez que tenga el archivo, puede extraer metadatos de él para obtener información sobre el software utilizado junto con su versión y ver si se pueden explotar las vulnerabilidades. Por este motivo, le recomendamos que tenga cuidado con los metadatos de sus documentos publicados e incluya la menor cantidad de información posible.

En resumen, es muy probable que este formato de archivo se utilice con fines maliciosos, como archivos adjuntos y exploits. Por lo tanto, es importante usarlos con precaución y tomar las precauciones de seguridad adecuadas al usarlos.
Al crear un archivo en este formato:

- Los productos de seguridad que pueden analizar y detener este tipo de amenazas son esenciales, especialmente para dispositivos que comparten información con clientes o personas desconocidas, ya que no se puede verificar la autenticidad de los editores de documentos.
- Si el software utilizado para abrir el PDF muestra un formulario que le pregunta si desea abrir el documento en cuestión, ejecutarlo o habilitar alguna función, es probable que sea un código malicioso y sea útil para verificar la corrección.
- Asegúrese de que el software utilizado para ver estos documentos esté actualizado a la última versión. Esto reduce el riesgo de ser víctima de archivos PDF que contienen vulnerabilidades.

REFERENCIAS

REFERENCIAS

- https://www.bbc.com/news/technology-65965453
- https://www.msn.com/en-us/news/technology/microsoft-azure-and-outlook-outages-were-caused-by-ddos-attacks/ar-AA1cKjin
- https://www.scmagazine.com/brief/incident-response/growing-cyber-threats-faced-by-submarine-cables
- https://www.securityweek.com/200000-wordpress-sites-exposed-to-attacks-exploiting-flaw-in-ultimate-member-plugin/?web_view=true
- https://telefonicatech.com/actualidad/bytehide-gana-la-startup-cloud-competition-proyecto-ciberseguridad-en-cloud
- https://telefonicatech.com/actualidad/1600-cest-good-tech-times-optimiza-tu-gasto-en-la-nube-con-aws-by-acens
- https://www.eleconomista.com.mx/tags/ciberseguridad
- https://esemanal.mx/2023/06/mexico-avanza-hacia-una-ley-de-ciberseguridad/

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