GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1524

En alianza con

TD SYNNEX FORTINET

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	0	2	2
MALWARE	1	2	1
NOTICIAS DE CIBERSEGURIDAD	0	0	4

VULNERABILIDADES

Vulnerabilidad crítica de seguridad descubierta en plugin popular de WordPress, LayerSlider

La vulnerabilidad, identificada como CVE-2024-2879, ha sido calificada con una puntuación CVSS de 9.8 sobre un máximo de 10.0. Se describe como un caso de inyección SQL que afecta a las versiones desde 7.9.11 hasta 7.10.0. Este problema ha sido abordado en la versión 7.10.1, lanzada el 27 de marzo de 2024, después de una divulgación responsable el 25 de marzo. Los mantenedores de LayerSlider mencionaron que "esta actualización incluye correcciones de seguridad importantes" en sus notas de lanzamiento.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/04/critical-security-flaw-found-in-popular.html

---

Ataque DoS a través de vulnerabilidad en protocolo HTTP/2

Un nuevo estudio ha revelado que el marco CONTINUATION del protocolo HTTP/2 puede ser explotado para llevar a cabo ataques de denegación de servicio (DoS). Esta técnica ha sido apodada como HTTP/2 CONTINUATION Flood por el investigador de seguridad, Bartek Nowotarski, quien notificó el problema al Centro de Coordinación CERT (CERT/CC) el 25 de enero de 2024 debido al riesgo potencial de ocasionar ataques de DoS masivos en todo Internet. Según Cloudflare Radar, el tráfico HTTP/2 representa aproximadamente el 60% de todo el tráfico HTTP generado por humanos (excluyendo bots).

Prioridad: 2 Urgente.

Ampliar información:

https://blog.segu-info.com.ar/2024/04/ataque-dos-traves-de-vulnerabilidad-en.html

---

CVE-2024-3158 sobre Chrome y sus marcadores

La utilización posterior a los marcadores en Google Chrome antes de la versión 123.0.6312.105 permitió a un atacante remoto explotar potencialmente la corrupción de almacenamiento a través de una página HTML diseñada, lo que resultó en una severidad de seguridad alta en Chrome.

Prioridad: 3 Importante.

Ampliar información:

https://packetstormsecurity.com/files/cve/CVE-2024-3158

Red Hat advierte sobre una puerta trasera en las herramientas XZ utilizadas por la mayoría de las distribuciones de Linux

Red Hat ha emitido una advertencia urgente a los usuarios, instando a que dejen de utilizar inmediatamente sistemas que ejecuten versiones de desarrollo y experimentales de Fedora. Esta advertencia surge debido a la detección de una puerta trasera en las últimas herramientas y bibliotecas de compresión de datos XZ Utils. La compañía declaró: "POR FAVOR, DEJEN DE USAR INMEDIATAMENTE CUALQUIER INSTANCIA DE FEDORA 41 O FEDORA RAWHIDE para trabajo o actividad personal". Esta acción preventiva es crucial para proteger la seguridad y la integridad de los sistemas afectados hasta que se resuelva completamente la situación.

Prioridad: 2 Urgente.

Ampliar información:

https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y aplicaciones actualizados conforme a información directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se pueden aplicar las actualizaciones necesarias de inmediato.
- Establecer una política y un plan periódico de mitigación de vulnerabilidades.

- Utilizar soluciones de gestión de vulnerabilidades para priorizar y abordar las vulnerabilidades.
- Adquirir tecnologías para bloquear accesos maliciosos y explotaciones de vulnerabilidades conocidas y de día cero.
- Utilizar servicios de Ethical Hacking para identificar posibles superficies de ciberataque y proteger los datos sensibles.
- Implementar sistemas de detección de intrusiones, sistemas de prevención de pérdida de datos y firewalls de aplicaciones web.
- Realizar auditorías de seguridad y pruebas de penetración regularmente.
- Educar a los usuarios y al personal de TI sobre las mejores prácticas de seguridad cibernética.
- Establecer políticas de seguridad sólidas, como el uso de contraseñas seguras y la gestión adecuada de accesos y privilegios.

MALWARE

El Malware para Android Vultur expande su alcance

Los autores del malware bancario para Android, Vultur, han sido detectados añadiendo nuevas características técnicas que permiten al operador del malware interactuar aún más remotamente con el dispositivo móvil de la víctima. Además, Vultur ha comenzado a disfrazar de forma más efectiva su actividad maliciosa mediante la encriptación de su comunicación C2, utilizando múltiples cargas útiles encriptadas que se descifran sobre la marcha. Estos cambios técnicos y tácticos hacen que Vultur sea más sigiloso, volviéndose difícil de detectar, lo que aumenta la preocupación sobre su capacidad para robar información confidencial y realizar actividades financieras no autorizadas en los dispositivos afectados.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.fox-it.com/2024/03/28/android-malware-vultur-expands-its-wingspan/

Aplicaciones maliciosas atrapadas convirtiendo teléfonos Android en Proxies para ciberdelincuentes, de forma secreta

El equipo de inteligencia de amenazas Satori de HUMAN ha descubierto varias aplicaciones maliciosas en la tienda Google Play Store que convierten los dispositivos móviles que ejecutan el sistema operativo Android en proxies residenciales (RESIPs) para otros actores de amenazas. Estas aplicaciones VPN están equipadas con una biblioteca Golang que transforma el dispositivo del usuario en un nodo proxy sin su conocimiento. Este operativo ha sido denominado PROXYLIB por la empresa. Las 29 aplicaciones maliciosas han sido eliminadas por Google.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/04/malicious-apps-caught-secretly-turning.html

---

Campaña masiva de phishing golpea a América Latina: RAT de Venom dirigido a múltiples sectores

El actor de amenazas conocido como TA558 ha sido identificado como responsable de una nueva campaña masiva de phishing que tiene como objetivo una amplia gama de sectores en América Latina con el fin de desplegar Venom RAT. Estos ataques se han dirigido principalmente a sectores como el hotelero, de viajes, comercio, financiero, manufacturero, industrial y gubernamental en países como España, México, Estados Unidos, Colombia, Portugal, Brasil, República Dominicana y Argentina.

Prioridad: 1 Critico.

Ampliar información:

https://thehackernews.com/2024/04/massive-phishing-campaign-strikes-latin.html

---

Nueva campaña de phishing dirigida a la industria petrolera y del gas con malware evolucionado para robar datos

Según el investigador de Cofense, Dylan Duncan, los correos electrónicos de phishing utilizan un señuelo único relacionado con un incidente vehicular. En etapas posteriores de la cadena de infección, falsifican al Federal Bureau of Transportation en un PDF que menciona una multa significativa por el incidente. El mensaje de correo electrónico incluye un enlace malicioso que aprovecha una falla de redirección abierta para dirigir a los destinatarios a un enlace que supuestamente aloja un documento PDF.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/04/new-phishing-campaign-targets-oil-gas.html

---

Recomendaciones generales sobre malware:

- Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
- Utilizar soluciones de seguridad confiables, como antivirus y firewalls, y mantenerlos actualizados.
- Implementar autenticación multifactor en cuentas y sistemas para agregar una capa adicional de seguridad.
- Educar a los usuarios sobre la importancia de no hacer clic en enlaces o adjuntos sospechosos en correos electrónicos o mensajes.

- Realizar copias de seguridad regulares de los datos importantes y guardarlas en un lugar seguro y fuera de línea.
- Evitar descargar software de fuentes no confiables y solo utilizar tiendas oficiales para obtener aplicaciones.
- Establecer políticas de contraseñas sólidas y cambiarlas regularmente.
- Limitar los privilegios de acceso para los usuarios y las cuentas, y solo otorgar los permisos necesarios.
- Monitorear de cerca la actividad de red y utilizar herramientas de detección de intrusiones.

NOTICIAS DE CIBERSEGURIDAD

El ataque Bypass para filtrado de correo electrónico en la nube funciona el 80% del tiempo

Los científicos informáticos han descubierto una configuración errónea sorprendentemente prevalente en los servicios de filtrado de correo no deseado en la nube para empresas, junto con un exploit para aprovecharla. Estos hallazgos revelan que las organizaciones están mucho más expuestas a amenazas cibernéticas basadas en correo electrónico de lo que creen. En un documento que se presentará en la próxima conferencia ACM Web 2024 en Singapur durante mayo, el equipo de investigación académica señaló que los servicios ampliamente utilizados de proveedores como Proofpoint, Barracuda, Mimecast, entre otros; podrían ser eludidos en al menos el 80% de los dominios principales que examinaron. Este descubrimiento resalta la necesidad de una mayor atención y medidas de seguridad robustas para proteger las organizaciones contra amenazas cibernéticas a través del correo electrónico.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/cloud-security/cloud-email-filtering-bypass-attack

---

La Junta de Seguridad Cibernética de EE. UU. critica a Microsoft por brecha a cargo de hackers con base en China

La Junta de Revisión de Seguridad Cibernética de EE. UU. (CSRB, por sus siglas en inglés) ha criticado a Microsoft por una serie de fallas de seguridad que llevaron a la brecha de casi dos docenas de empresas en Europa y EE. UU. por parte de un grupo estatal chino llamado Storm-0558, el año pasado. Estos hallazgos, publicados por el Departamento de Seguridad Nacional (DHS) el martes, encontraron que la intrusión era prevenible y que tuvo éxito debido a una "cascada de errores evitables de Microsoft". El DHS declaró en un comunicado que identificó una serie de decisiones operativas y estratégicas de Microsoft que, en conjunto, apuntaban a una cultura corporativa que relegaba las inversiones en seguridad empresarial y una gestión de riesgos rigurosa.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/04/us-cyber-safety-board-slams-microsoft.html

---

AT&T confirma robo de 73 millones de datos de clientes

AT&T ha confirmado que ha sido víctima de una violación de datos que afecta a 73 millones de clientes. Esta admisión llega después de que la compañía negara repetidamente durante las últimas dos semanas que una gran cantidad de datos filtrados provinieran de ellos o que sus sistemas hubieran sido vulnerados. A pesar de mantener que no hay evidencia de que sus sistemas hayan sido comprometidos, AT&T ha reconocido que los datos filtrados pertenecen a 73 millones de clientes, tanto actuales como anteriores.

Prioridad: 3 Importante.

Ampliar información:

https://blog.segu-info.com.ar/2024/04/at-confirma-robo-de-73-millones-de.html

---

Nuevo ransomware SEXi, activo en Latinoamérica

El proveedor chileno de hosting IxMetro Powerhost fue víctima de un ciberataque perpetrado por una nueva banda de ransomware conocida como SEXi. Este ataque resultó en el cifrado de los servidores y copias de seguridad VMware ESXi de la compañía. El lunes, la división chilena de PowerHost, IxMetro, notificó a sus clientes sobre un ataque de ransomware ocurrido durante la madrugada del sábado. Este ataque afectó algunos de los servidores VMware ESXi de la compañía, los cuales se utilizan para alojar servidores privados virtuales para los clientes.

Prioridad: 3 Importante.

Ampliar información:

https://blog.segu-info.com.ar/2024/04/nuevo-ransomware-sexi-activo-en.html

---