GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2823

En alianza con

TD SYNNEX FORTINET

BOLETIN DE CIBERINTELIGENCIA DE AMENAZAS

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	3	1	
MALWARE	1	2	1
NOTICIAS DE CIBERSEGURIDAD	1	2	3
SECTOR FINANCIERO	1		

VULNERABILIDADES

Herramienta de conferencia web Apache OpenMeetings expuesta a vulnerabilidades críticas

Se han encontrado múltiples vulnerabilidades en Apache OpenMeetings, una solución de conferencias web, que podrían permitir a atacantes tomar el control de cuentas de administración y ejecutar código malicioso en servidores vulnerables. Las vulnerabilidades han sido abordadas en una actualización reciente, pero antes de eso, los atacantes podían explotar estas fallas para obtener acceso no autorizado a cuentas de usuario y obtener privilegios de administrador, lo que les permitiría realizar cambios en la instancia de OpenMeetings y ejecutar comandos de shell arbitrarios.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.sonarsource.com/blog/a-twist-in-the-code-openmeetings-vulnerabilities-through-unexpected-application-state/

Vulnerabilidades de Adobe ColdFusion

Adobe emitió alertas sobre tres vulnerabilidades en su producto ColdFusion. A pesar de lanzar parches, las vulnerabilidades aún están siendo explotadas en la web. Se recomienda a los usuarios de ColdFusion seguir las actualizaciones de Adobe y aplicar los parches para protegerse contra posibles riesgos de seguridad.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.natlawreview.com/article/patch-adobe-coldfusion-vulnerabilities-being-exploited-wild-asap

---

Vulnerabilidad CVE-2023-3519 de CITRIX/NETSCALER puede causar más daño del imaginado

La Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA) emitió una advertencia sobre una vulnerabilidad conocida como CVE-2023-3519 en Citrix/NetScaler, que afecta a Citrix ADC y Citrix Gateway. Los actores de amenazas intentaron atacar la infraestructura crítica utilizando esta vulnerabilidad, pero no tuvieron éxito debido a las defensas y segmentación de la red.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.cibertip.com/ciberseguridad/cve-2023-3519-de-citrix-netscaler-puede-causar-mas-dano-de-lo-que-uno-puede-imaginar/
- https://bishopfox.com/blog/citrix-adc-gateway-rce-cve-2023-3519

Vulnerabilidades en Microsoft Edge (CVE-2023-35392, CVE-2023-38187, CVE-2023-38173)

Se detallan tres vulnerabilidades encontradas en el navegador web Microsoft Edge, identificadas como CVE-2023-35392, CVE-2023-38187 y CVE-2023-38173. Estas vulnerabilidades afectan la seguridad del navegador y podrían permitir a actores de amenazas remotos ejecutar código malicioso, obtener información sensible o causar un mal funcionamiento del sistema. Se recomienda a los usuarios y administradores aplicar los parches de seguridad proporcionados por Microsoft para mitigar los riesgos asociados con estas vulnerabilidades.

Prioridad: 2 Urgente.

Ampliar información:

- https://vulmon.com/vulnerabilitydetails?qid=CVE-2023-35392
- https://vulmon.com/vulnerabilitydetails?qid=CVE-2023-38187
- https://vulmon.com/vulnerabilitydetails?qid=CVE-2023-38173

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 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

FIN8 usa Backdoor Sardonic modificada para distribuir el ransomware BlackCat

El grupo de amenazas financieras conocido como FIN8 ha sido observado utilizando una versión "renovada" de la puerta trasera llamada Sardonic para distribuir el ransomware BlackCat. Symantec informó que este desarrollo es un intento del grupo de delitos electrónicos por diversificar su enfoque y maximizar ganancias de entidades infectadas.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/07/fin8-group-using-modified-sardonic.html

---

HotRat: Nueva variante del malware AsyncRAT que se propaga a través de software pirateado

Una nueva variante del malware AsyncRAT, llamada HotRat, se está distribuyendo a través de versiones gratuitas y piratas de software popular y utilidades como videojuegos, software de edición

de imágenes y sonido, y Microsoft Office. HotRat permite a los atacantes robar credenciales de inicio de sesión, billeteras de criptomonedas, capturar pantallas, registrar pulsaciones de teclas, instalar más malware y acceder o alterar datos del portapapeles. Los atacantes utilizan un script de AutoHotkey malicioso para infectar sistemas a través de software pirateado, lo que permite desactivar soluciones antivirus y lanzar el payload de HotRat mediante un cargador de Visual Basic Script. Es importante destacar que este ataque requiere privilegios administrativos para lograr sus objetivos y resalta los riesgos asociados con la descarga de software ilegal.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/07/hotrat-new-variant-of-asyncrat-malware.html
- https://decoded.avast.io/martinchlumecky/hotrat-the-risks-of-illegal-software-downloads-and-hidden-autohotkey-script-within/

Nuevo gusano P2PInfect dirigido a servidores Redis en sistemas Linux y Windows

Investigadores de ciberseguridad descubrieron el gusano P2PInfect, que ataca servidores vulnerables de Redis en sistemas Linux y Windows. Utiliza una vulnerabilidad de escape de sandbox de Lua para propagarse. Una vez dentro, establece una red P2P para infectar otros hosts expuestos de Redis y SSH. El objetivo final no está claro, pero podría prepararse para un ataque más sofisticado. Los usuarios de Redis deben actualizar y tomar medidas de seguridad.

Prioridad: 2 Urgente.

Ampliar información:

- https://unit42.paloaltonetworks.com/peer-to-peer-worm-p2pinfect/

Nuevo software espía WyrmSpy y DragonEgg

Se ha descubierto un nuevo spyware para Android llamado WyrmSpy y DragonEgg, vinculado al grupo de ciberespionaje chino APT41. Estas variantes sofisticadas han estado recopilando datos de usuarios, incluidas fotos y mensajes, y se conectan a un servidor de comando y control. Este hallazgo destaca la creciente amenaza del malware avanzado en dispositivos móviles.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/07/chinese-apt41-hackers-target-mobile.html
- https://www.lookout.com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41

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

Técnica de falsificación de tokens de Azure AD en Microsoft se extiende más allá de Outlook

Según la empresa de seguridad en la nube Wiz, el ataque reciente del actor estatal chino conocido como Storm-0558 contra la infraestructura de correo electrónico de Microsoft tiene un alcance más amplio de lo que se pensaba. Además de falsificar tokens de Azure Active Directory (AAD) para obtener acceso no autorizado a Outlook Web Access (OWA) y Outlook.com, el atacante también podría haber falsificado tokens de acceso para otras aplicaciones de Azure AD, incluidas OneDrive, SharePoint, Teams y aplicaciones de terceros que utilizan "Iniciar sesión con Microsoft". Esto otorga al atacante un acceso poderoso a una amplia variedad de aplicaciones y servicios de Microsoft, lo que lo convierte en un riesgo significativo para las organizaciones afectadas.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/07/azure-ad-token-forging-technique-in.html
- https://thehackernews.com/2023/07/microsoft-bug-allowed-hackers-to-breach.html

---

Botnets DDoS secuestran dispositivos Zyxel para lanzar ataques devastadores

Botnets de DDoS están aprovechando una vulnerabilidad crítica en dispositivos Zyxel para obtener el control remoto de sistemas vulnerables. La falla CVE-2023-28771 permite la ejecución de código arbitrario y ha sido utilizada para crear botnets capaces de realizar ataques DDoS. Los ataques han sido detectados en múltiples regiones y afectan a variantes de Mirai y un botnet llamado Katana. También se ha observado un aumento en la sofisticación de los ataques DDoS, con tácticas como ataques de lavado DNS y el uso de botnets de máquinas virtuales. Además, grupos hacktivistas pro-rusos como KillNet, REvil y Anonymous Sudan han estado dirigiendo sus ataques principalmente hacia objetivos en EE. UU. y Europa. La estructura de KillNet ha estado cambiando para atraer más atención de los medios y aumentar su influencia en las operaciones.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/07/ddos-botnets-hijacking-zyxel-devices-to.html

---

VirusTotal se disculpa por fuga de datos que afecta a 5.600 clientes

VirusTotal se disculpa por una filtración de datos que afectó a más de 5,600 clientes. Un empleado subió por error un archivo CSV a la plataforma el mes pasado, exponiendo los nombres y correos electrónicos corporativos de los clientes con cuentas Premium. El incidente fue causado por un error humano y no fue resultado de un ataque cibernético o vulnerabilidad en VirusTotal. El archivo filtrado solo fue accesible para socios y analistas de ciberseguridad con cuentas Premium en la plataforma. La información filtrada incluía cuentas vinculadas a agencias gubernamentales en EE. UU., Alemania, Países Bajos, Taiwán y Reino Unido, incluyendo el Cyber Command, FBI y NSA de EE. UU. VirusTotal eliminó el archivo de la plataforma una hora después de su publicación.

Prioridad: 3 Importante.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/virustotal-apologizes-for-data-leak-affecting-5-600-customers/

RED TEAM vs BLUE TEAM vs PURPLE TEAM

Los equipos Rojos (Red Teams) emulan a los atacantes para encontrar vulnerabilidades en las defensas de una organización. Los equipos Azules (Blue Teams) se dedican a defenderse de los ataques y mejorar la seguridad. Los equipos Púrpura (Purple Teams) actúan como consejeros, integrando tácticas y controles defensivos de los Azules con las amenazas detectadas por los Rojos. Es esencial que haya una colaboración y retroalimentación entre los equipos para mejorar

continuamente la postura de seguridad. Los equipos Rojo y Azul deben trabajar juntos para maximizar los resultados en lugar de depender de una entidad adicional como el Equipo Púrpura.

Prioridad: 3 Importante.

Ampliar información:

- https://esgeeks.com/red-team-vs-blue-team-vs-purple-team/?feed_id=18397&_unique_id=64bb010b33f98

Google evitó un ciberataque de altas dimensiones a través de la nube

Google pudo evitar un ciberataque de gran magnitud gracias a la respuesta rápida y efectiva de su sistema en la nube. El ataque DDoS recibió 46 millones de solicitudes por segundo, pero la nube detectó y bloqueó el tráfico malintencionado, evitando así que el ataque tuviera éxito. La nube ofrece ventajas de ciberseguridad, como automatización, monitoreo y la capacidad de anticiparse a las amenazas. Google ha realizado adquisiciones en empresas de ciberseguridad para fortalecer su tecnología y mejorar su capacidad de prevenir y defenderse de ciberataques. Las empresas deben analizar qué modelo de ciberseguridad se adapta mejor a sus necesidades, ya sea basado en la nube, convencional o mixto.

Prioridad: 3 Importante.

Ampliar información:

- https://www.infobae.com/tecno/2023/07/21/como-google-evito-un-ciberataque-de-altas-dimensiones-usando-la-nube/?utm_medium=Social&utm_source=Twitter#Echobox=1689965519

---

325 aplicaciones infectadas en Android

Se han identificado 325 aplicaciones infectadas en dispositivos Android que los usuarios deben borrar de inmediato para evitar riesgos como robo de datos, dinero y daños en sus dispositivos. Algunas de estas aplicaciones se hacen pasar por herramientas de seguridad de entidades

bancarias y roban datos bancarios automáticamente. Otras aplicaciones se esconden bajo la apariencia de juegos y también pueden robar datos personales y bancarios. Además, se han detectado aplicaciones con el troyano Android.Spy.SpinOk que ralentiza los dispositivos y puede robar información. Se aconseja a los usuarios tener cuidado al descargar aplicaciones y evitar instalar cualquier cosa fuera de Google Play. Además, se recomienda contar con un antivirus para protegerse de futuros riesgos.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.movilzona.es/noticias/ofertas/aliexpress-moviles-nothing-phone-1-0723/