GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4123

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín de ciberseguridad semanal 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, tecnología y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	6		
MALWARE	2	3	
NOTICIAS DE CIBERSEGURIDAD		2	2

VULNERABILIDADES

Vulnerabilidades Críticas en CasaOS Cloud Software

Dos vulnerabilidades críticas descubiertas en el software de nube personal de código abierto CasaOS podrían ser explotadas por atacantes para ejecutar código arbitrario y tomar el control de sistemas susceptibles. Las vulnerabilidades, conocidas como CVE-2023-37265 y CVE-2023-37266, tienen una puntuación CVSS de 9.8 sobre 10. Estas fallas permiten a los atacantes eludir los requisitos de autenticación y obtener acceso completo al panel de CasaOS. Además, el soporte de CasaOS para aplicaciones de terceros podría ser utilizado para ejecutar comandos arbitrarios en el sistema y ganar acceso persistente.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/10/critical-vulnerabilities-uncovered-in.html

---

Vulnerabilidad Zero-Day en Citrix NetScaler Explotada Desde Agosto

La CVE-2023-4966, una vulnerabilidad crítica en Citrix NetScaler, se ha explotado como zero-day desde agosto, permitiendo la filtración de datos sin autenticación. Aunque Citrix emitió parches el 10 de octubre, se advierte sobre la explotación en curso y se recomienda a los usuarios que actualicen sus sistemas de inmediato. Mandiant, informa que la vulnerabilidad se ha utilizado en ataques dirigidos a gobiernos, servicios profesionales y organizaciones tecnológicas, lo que posibilita el secuestro de sesiones autenticadas y el acceso no autorizado a recursos.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/recent-netscaler-vulnerability-exploited-as-zero-day-since-august/

Oracle Publica Parches para Resolver 185 Vulnerabilidades en su CPU

Oracle ha lanzado 387 nuevos parches de seguridad como parte de su CPU de octubre de 2023 para abordar vulnerabilidades que afectan a su propio código y componentes de terceros. Más de 40 de estos parches solucionan fallos de gravedad crítica y más de 200 resuelven errores que pueden ser explotados de forma remota sin autenticación. Los productos de Oracle con la mayor cantidad de parches son las aplicaciones de servicios financieros, seguidos de Comunicaciones de Oracle, Fusion Middleware y MySQL, entre otros. La empresa insta a sus clientes a aplicar estos parches de seguridad de inmediato debido a la amenaza que representan los ataques exitosos.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/oracle-patches-185-vulnerabilities-with-october-2023-cpu/?web_view=true

---

Vulnerabilidad de Divulgación de Información Sensible en Sophos Firewall

Sophos Firewall ha identificado una vulnerabilidad que permite a un usuario remoto provocar la divulgación de información sensible en el sistema de destino. Esta vulnerabilidad afecta a versiones anteriores a Sophos Firewall v19.5 MR3 (19.5.3). Se recomienda aplicar las soluciones proporcionadas por el vendedor para abordar esta vulnerabilidad. Para obtener más detalles y correcciones, visite el sitio web del proveedor o siga el enlace proporcionado. No se requiere ninguna acción para los clientes de Sophos Firewall que tengan habilitada la función de instalación automática de parches. El identificador de la vulnerabilidad es CVE-2023-5552.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.hkcert.org/security-bulletin/sophos-firewall-sensitive-information-disclosure-vulnerability_20231019/

Múltiples Vulnerabilidades en ChromeOS

Se han identificado múltiples vulnerabilidades en ChromeOS que podrían ser explotadas por un atacante remoto para provocar la divulgación de información sensible, condiciones de denegación de servicio y ejecución de código remoto en el sistema de destino. Estas vulnerabilidades afectan a versiones anteriores a 118.0.5993.86 (Versión de la plataforma: 15604.45.0). Se recomienda aplicar las correcciones proporcionadas por el proveedor. Para obtener más detalles y correcciones, visite el sitio web del proveedor o siga el enlace proporcionado. No se dispone de información CVE específica para estas vulnerabilidades.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.hkcert.org/security-bulletin/chromeos-multiple-vulnerabilities_20231019

Múltiples Vulnerabilidades en Apache HTTP Server

Se han identificado múltiples vulnerabilidades en Apache HTTP Server que podrían ser explotadas por un atacante remoto para provocar una denegación de servicio y la divulgación de información sensible en el sistema de destino. Estas vulnerabilidades afectan a versiones anteriores a Apache HTTP Server 2.4.58. Se recomienda aplicar las correcciones proporcionadas por el proveedor. Las vulnerabilidades tienen los siguientes identificadores CVE: CVE-2023-31122, CVE-2023-43622 y CVE-2023-45802.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.hkcert.org/security-bulletin/apache-http-server-multiple-vulnerabilities_20231020

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

MATA Malware Explota EDR en Ataques a Empresas de Defensa

MATA, una puerta trasera actualizada, se ha utilizado en ataques a empresas de petróleo, gas y la industria de defensa en Europa del Este entre agosto de 2022 a mayo de 2023. Los atacantes emplearon correos electrónicos de spear-phishing y una vulnerabilidad de Internet Explorer (CVE-2021-26411) para iniciar la infección. MATA combina un cargador, un troyano principal así como un ladrón de información para obtener acceso a las redes objetivo. Estos ataques exploraron las debilidades de soluciones de cumplimiento de seguridad, abusando de las soluciones EDR para distribuir malware en la red corporativa. Las últimas versiones de MATA incluyen una amplia variedad de comandos para el control remoto y la ejecución de acciones maliciosas.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/mata-malware-framework-exploits-edr-in-attacks-on-defense-firms/

Malware Oculto en Falsas Actualizaciones de Navegadores

Los ciberdelincuentes están escondiendo malware en notificaciones falsas de actualización a navegadores en sitios web legítimos pero vulnerables. Los atacantes utilizan JavaScript malicioso para engañar a los usuarios, quienes, al hacer clic en "Actualizar", descargan malware en sus

computadoras. Se insta a los usuarios a ser cautelosos, verificando cualquier actualización de navegador a través de fuentes confiables para evitar caer en esta trampa.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.darkreading.com/threat-intelligence/watch-out-attackers-hiding-malware-browser-updates

---

Malvertising Engañoso Utiliza Punycode para Suplantar el Sitio de KeePass

Atacantes han registrado un dominio falso que utiliza el código Punycode para suplantar el sitio real de KeePass. Cuando los usuarios hacen clic en un anuncio de Google que parece legítimo, son redirigidos al dominio falso. Desde allí, los usuarios que intentan descargar KeePass obtienen un instalador malicioso con una firma digital válida. Este instalador contiene código malicioso que se comunica con un servidor de comando y control y puede permitir futuras actividades de amenaza. Por lo tanto, el sitio falso se utiliza para distribuir malware a los usuarios que buscan descargar el software KeePass genuino.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.malwarebytes.com/blog/threat-intelligence/2023/10/clever-malvertising-attack-uses-punycode-to-look-like-legitimate-website?&web_view=true

---

ExelaStealer: Nuevo Malware de Robo de Información que Gana Terreno en la Dark Web

Se ha descubierto un nuevo malware de robo de información llamado ExelaStealer que apareció en agosto. Tiene la capacidad de robar datos sensibles de sistemas Windows, como contraseñas y

detalles de tarjetas de crédito. Se encuentra disponible en dos variantes, una de código abierto y otra de pago, con el código fuente disponible de forma gratuita. Aunque el método de infección inicial es desconocido, a través de phishing pueden realizarse ataques a sitios web o mediante otros malware.

Prioridad: 2 Urgente.

Ampliar información:

- https://cyware.com/news/exelastealer-a-new-info-stealer-gaining-traction-on-dark-web-a16a4022/?web_view=true

---

Hackers Explotan Códigos QR con QRLJacking para Distribuir Malware

Los hackers están aprovechando los códigos QR para realizar ataques de phishing y distribuir malware, utilizando métodos como QRLJacking y Quishing. QRLJacking implica la creación de sitios de phishing para engañar a las víctimas con el fin de robar datos sensibles cuando escanean códigos QR maliciosos. Para protegerse, es importante escanear códigos QR solo desde fuentes confiables, verificar las URL de destino antes de escanear, además de mantener el software antivirus actualizado y realizar auditorías de seguridad en organizaciones.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.hackread.com/hackers-exploit-qr-codes-qrljacking-malware/?web_view=true

---

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

OpenSSF Lanza Repositorio de Paquetes Maliciosos

La Open Source Security Foundation (OpenSSF) ha introducido el Repositorio de Paquetes Maliciosos, con más de 15,000 informes, para combatir los crecientes ciberataques que aprovechan paquetes de código abierto y reforzar la seguridad en estos ecosistemas. Este repositorio se ha convertido en un recurso esencial para la protección e integridad del software de código abierto.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.hackread.com/openssf-launches-malicious-packages-repository/?web_view=true

---

Okta informa que su sistema de soporte fue vulnerado mediante el uso de credenciales robadas

Okta informó que su sistema de soporte fue vulnerado por atacantes que accedieron a archivos que contenían cookies y tokens de sesión cargados por los clientes. Esta violación de seguridad no afectó los servicios de producción de Okta. Además, Cloudflare descubrió actividad maliciosa relacionada con la violación en sus servidores y ambas compañías tomaron medidas para abordar el incidente. No está claro cuántos clientes se vieron afectados ni cuándo ocurrió la violación.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/okta-says-its-support-system-was-breached-using-stolen-credentials/

Europol desmantela la infraestructura de ransomware Ragnar Locker y arresta a su desarrollador clave

Europol anunció la desarticulación de la infraestructura relacionada con el ransomware Ragnar Locker y el arresto de un "objetivo clave" en Francia. Este grupo de ransomware, conocido por su táctica de doble extorsión, ha atacado a 168 empresas internacionales en todo el mundo desde 2020. Las autoridades de varios países coordinaron esfuerzos para llevar a cabo estas acciones contra el grupo y sus miembros, incluido el arresto de su desarrollador principal en Francia.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/10/europol-dismantles-ragnar-locker.html

---

Un Actor de Amenazas Vende Acceso al Portal de la Policía de Facebook e Instagram

Un actor de amenazas está vendiendo acceso al Portal de la Policía de Facebook e Instagram, utilizado por las agencias de aplicación de la ley para solicitar datos relacionados con usuarios bajo

investigación. El acceso se ofrece por $700 y puede tener más de una cuenta existente en el portal. Especulan que Meta fue víctima de un ataque de ingeniería social que engañó a un empleado para dar a los atacantes acceso al portal o que el actor de amenazas tenía credenciales de una cuenta legítima de aplicación de la ley. Este acceso podría ser abusado para realizar solicitudes de datos no autorizadas, habilitar el acoso, doxxing, llevar a cabo acciones falsas de aplicación de la ley, corriendo el riesgo de robo de identidad, lo que plantea serias preocupaciones de privacidad y seguridad para los usuarios.

Prioridad: 3 Importante.

Ampliar información:

- https://securityaffairs.com/152811/cyber-crime/facebook-and-instagrams-police-portal-access.html