GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2923

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	2	1	
MALWARE	1	3	
NOTICIAS DE CIBERSEGURIDAD		3	2

VULNERABILIDADES

Zimbra parchea vulnerabilidad de día cero explotada en ataques XSS

Zimbra ha lanzado actualizaciones de seguridad para corregir una vulnerabilidad de día cero explotada en ataques a servidores de correo electrónico Zimbra Collaboration Suite (ZCS). La vulnerabilidad XSS, conocida como CVE-2023-38750, fue descubierta por un investigador de Google. La CISA ha advertido a las agencias federales de EE. UU. que deben parchear antes del 17 de agosto. Se insta a las empresas privadas a priorizar las actualizaciones para todas las vulnerabilidades en el catálogo de vulnerabilidades explotadas de la CISA.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/zimbra-patches-zero-day-vulnerability-exploited-in-xss-attacks/?&web_view=true

Falla del complemento WordPress Ninja Forms permite a los piratas informáticos robar los datos enviados

El complemento de creación de formularios de WordPress, Ninja Forms, tiene tres vulnerabilidades que permiten a los hackers robar datos de usuarios y obtener privilegios elevados. Los investigadores de Patchstack informaron de las vulnerabilidades el 22 de junio de 2023, el desarrollador lanzó una actualización (versión 3.6.26) el 4 de julio de 2023. Sin embargo, aún hay unos 400,000 sitios vulnerables debido a que muchos usuarios no han actualizado. Se recomienda a los administradores actualizar el complemento lo antes posible o desactivarlo hasta que se pueda aplicar el parche.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/wordpress-ninja-forms-plugin-flaw-lets-hackers-steal-submitted-data/?&web_view=true

Múltiples vulnerabilidades en productos de Aruba

Se han identificado múltiples vulnerabilidades en los Productos de Aruba, que representan un riesgo medio. Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para ejecutar código de forma remota y acceder a información sensible en el sistema objetivo. Las versiones de software afectadas incluyen ArubaOS 10.4.0.1 y anteriores, así como varias versiones de InstantOS. Es fundamental que los usuarios apliquen las correcciones proporcionadas por Aruba para solucionar estas vulnerabilidades. Algunas versiones en estado de Fin de Vida también se ven afectadas y no son parcheadas por este aviso. Para obtener más información y acceder a las correcciones, los usuarios deben visitar el sitio web oficial de Aruba. Las vulnerabilidades están identificadas por los siguientes números CVE: CVE-2022-25667, CVE-2023-35980, CVE-2023-35981 y CVE-2023-35982.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.hkcert.org/security-bulletin/aruba-products-multiple-vulnerabilities_20230726

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

Nuevo malware de Android usa OCR para robar credenciales de imágenes

Trend Micro encontró que los malwares 'CherryBlos' y 'FakeTrade' para Android roban credenciales de criptomonedas y realizan estafas. CherryBlos usa OCR para extraer frases de recuperación de billeteras. Google eliminó las apps maliciosas, pero usuarios afectados pueden requerir limpieza manual de sus dispositivos. Mantener precaución al instalar aplicaciones es crucial para evitar estas amenazas.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/new-android-malware-uses-ocr-to-steal-credentials-from-images/

Nuevo malware Nitrogen lanzado a través de Google Ads para ataques de ransomware

La campaña de malware 'Nitrogen' utiliza anuncios en Google y Bing para promover sitios web falsos que infectan a usuarios desprevenidos con cargas útiles de Cobalt Strike y ransomware. El objetivo del malware es proporcionar a los atacantes acceso inicial a redes corporativas para robar datos, realizar ciberespionaje y, en última instancia, desplegar el ransomware BlackCat/ALPHV. Se dirige principalmente a organizaciones tecnológicas y sin fines de lucro en América del Norte, haciendo uso de aplicaciones populares como AnyDesk, Cisco AnyConnect VPN, TreeSize Free y WinSCP como señuelos. Se recomienda evitar hacer clic en resultados "promocionados" al descargar software y solo descargar desde sitios oficiales de los desarrolladores.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/new-nitrogen-malware-pushed-via-google-ads-for-ransomware-attacks/

El malware Decoy Dog evoluciona para expandir su alcance

El malware Decoy Dog está evolucionando y expandiendo su alcance en una nueva campaña de hackeo. Aunque su origen es incierto, se han detectado dominios sospechosos con conexiones a direcciones IP rusas. Más de 100 dispositivos están infectados y se han rastreado 21 dominios relacionados con el malware. Decoy Dog ha mejorado su funcionalidad desde su descubrimiento en abril, y se recomienda bloquear las direcciones IP relacionadas para mantenerse seguro. Aún se desconoce su propósito y los responsables detrás de la campaña.

Prioridad: 2 Urgente.

Ampliar información:

- https://cyware.com/news/decoy-dog-malware-evolves-to-expand-its-reach-015a4ea3/?web_view=true

---

macOS bajo ataque: examinando la creciente amenaza y las perspectivas de los usuarios

La amenaza de malware hacia macOS está en aumento, y los hackers están específicamente dirigidos a sistemas Mac. Ataques como "Geacon" Cobalt Strike, MacStealer y CloudMensis han comprometido la seguridad y privacidad de los usuarios de Apple. A pesar de esto, muchos usuarios de Mac todavía subestiman su ciberseguridad y mantienen mitos como que macOS es inmune a malware.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/07/macos-under-attack-examining-growing.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

Una guía paso a paso para parchear vulnerabilidades de software

El índice de amenazas cibernéticas de Coalition predice un aumento del 13% en la tasa promedio de vulnerabilidades y exposiciones comunes (CVE) para 2023. Ante el gran número de parches y actualizaciones mensuales, las organizaciones enfrentan dificultades en la gestión de parches. Para simplificar el proceso, se sugiere priorizar las actualizaciones según su gravedad y exposición. Luego, realizar pruebas exhaustivas para evitar interrupciones en el sistema. Además, es fundamental evaluar el ancho de banda del sistema para evitar sobrecargas. Seguir las mejores prácticas de gestión del cambio y utilizar un calendario de gestión de parches para implementar de manera segura también es clave. Evitar prácticas riesgosas como otorgar a los usuarios derechos de administrador y confiar en herramientas gratuitas que pueden no brindar la seguridad adecuada.

Con enfoque y planificación, las organizaciones pueden fortalecer su protección y reducir la vulnerabilidad frente a las amenazas cibernéticas.

Prioridad: 3 Importante.

Ampliar información:

- https://www.helpnetsecurity.com/2023/07/27/patch-management-guide/?web_view=true

---

Gmail tiene una nueva función contra las estafas

La función 'Navegación segura mejorada' de Google, anteriormente disponible en Chrome, ha sido implementada en Gmail para brindar una capa adicional de seguridad a los usuarios contra estafas y amenazas en línea. Al activar esta función, los usuarios recibirán advertencias antes de que se produzcan posibles amenazas, lo que les permitirá proteger sus credenciales y datos personales de manera más efectiva. Los usuarios pueden seguir unos simples pasos para activar esta protección en su cuenta de Gmail, lo que les permitirá navegar de manera más segura en la web y protegerse contra sitios, descargas y extensiones potencialmente peligrosas. Con esta nueva función, Google busca reforzar la seguridad de sus usuarios y brindarles mayor tranquilidad al utilizar su servicio de correo electrónico.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.genbeta.com/a-fondo/gmail-tiene-nueva-funcion-estafas-como-activar-navegacion-segura-mejorada-gratis-minuto

---

Protección de DNS: una defensa imprescindible contra los ataques cibernéticos

La Protección DNS es una importante estrategia de ciberseguridad que protege el Sistema de Nombres de Dominio de amenazas en línea. Es esencial para cualquier empresa que use internet, ya

que previene ataques de phishing y distribución de malware. Implementar DNS Protection mejora la seguridad de la organización, evita pérdidas de datos y mantiene el funcionamiento de la red sin interrupciones.

Prioridad: 2 Urgente.

Ampliar información:

- https://heimdalsecurity.com/blog/dns-protection/

La OTAN investiga presunto robo de datos por parte de SiegedSec

El grupo de hackers SiegedSec está siendo investigado por la OTAN debido a un presunto robo de datos en el Portal de Cooperación de Comunidades de Interés (COI). SiegedSec afirma haber robado cientos de documentos del portal y compartió parte de la información en Telegram. La filtración contiene datos de más de 8,000 usuarios, incluyendo nombres completos, direcciones de correo electrónico, títulos laborales y más. Se cree que el ataque afecta a 31 naciones miembros de la OTAN. Aunque SiegedSec no parece tener motivaciones financieras, su acción se asemeja más a la de hacktivistas, que buscan filtrar datos y hacer una declaración en lugar de obtener beneficios económicos. El grupo menciona que el ataque es en protesta a los ataques de los países miembros de la OTAN contra los derechos humanos.

Prioridad: 3 Importante.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/nato-investigates-alleged-data-theft-by-siegedsec-hackers/?&web_view=true

---

El sector educativo tiene la mayor proporción de víctimas de ransomware

Un nuevo informe de Sophos revela que el sector educativo tuvo el mayor número de víctimas de ransomware en 2022. Según el informe, el 79% de las instituciones de educación superior y el 80% de las instituciones de educación básica fueron comprometidas por ransomware durante el último año, lo que representa un aumento significativo con respecto a 2021. Se encontró que los exploits y las credenciales comprometidas fueron responsables del 77% de los ataques contra instituciones de educación superior y el 65% de los ataques contra instituciones de educación básica. Además, el sector educativo mostró una de las tasas más altas de pago de rescate, con un 56% de las víctimas de educación superior y un 47% de las escuelas que pagaron el rescate. Los expertos instan a las instituciones educativas a implementar MFA para protegerse contra futuros ataques de ransomware.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.infosecurity-magazine.com/news/education-sector-highest/?&web_view=true