GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1924

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	3
MALWARE	0	2	5
NOTICIAS DE CIBERSEGURIDAD	0	0	4

VULNERABILIDADES

Cuatro Vulnerabilidades Críticas de Ejecución Remota (RCE) en ArubaOS

HPE Aruba Networking ha emitido su aviso de seguridad de abril de 2024 detallando vulnerabilidades críticas de ejecución remota de código (RCE) que afectan a múltiples versiones de ArubaOS, su sistema operativo de red propietario. El aviso enumera diez vulnerabilidades, cuatro de las cuales son problemas de desbordamiento de búfer no autenticados de gravedad crítica (CVSS v3.1: 9.8) que pueden conducir a la ejecución remota de código (RCE). Los productos afectados por las fallas recién reveladas son: HPE Aruba Networking Mobility Conductor, Mobility Controllers, WLAN Gateways y SD-WAN Gateways gestionados por Aruba Central. ArubaOS 10.5.1.0 y versiones anteriores, 10.4.1.0 y anteriores, 8.11.2.1 y versiones anteriores, junto con 8.10.0.10 y anteriores.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/hpe-aruba-networking-fixes-four-critical-rce-flaws-in-arubaos/

Inyección de plantillas en el lado del servidor (SSTI) de CrushFTP

El equipo de investigación de amenazas de SonicWall Capture Labs se percató de una vulnerabilidad de inyección de plantillas en el lado del servidor no autenticada dentro de CrushFTP, evaluó su impacto y desarrolló medidas de mitigación. CrushFTP es una herramienta empresarial de transferencia de archivos. Herramientas similares han recibido una mayor atención por parte de los atacantes en los últimos años. Esta vulnerabilidad, CVE-2024-4040, tiene un puntaje CVSS de 10.0 y se ha informado que está siendo explotada en la naturaleza por CISA.

Prioridad: 3 Importante.

Ampliar información:

https://blog.sonicwall.com/en-us/2024/05/crushftp-server-side-template-injection-ssti/

Judge0 Sandbox Escape

Judge0 es un servicio de código abierto utilizado para ejecutar código arbitrario dentro de un sandbox seguro. El sitio web de Judge0 enumera 23 clientes que utilizan el servicio, con más de 300 instancias autohospedadas disponibles en Internet público y potencialmente muchas más dentro de redes internas. Security reveló vulnerabilidades en Judge0 que permiten a un adversario con acceso suficiente realizar un escape de sandbox y obtener

permisos de root en la máquina host. Estas vulnerabilidades fueron asignadas a CVE-2024-29021, CVE-2024-28185 y CVE-2024-28189

Prioridad: 3 Importante.

Ampliar información:

https://www.infosecurity-magazine.com/news/judge0-sandbox-flaws-systems/

Vulnerabilidad en la deserialización de "R"

Los investigadores de HiddenLayer han descubierto una vulnerabilidad, CVE-2024-27322, en el lenguaje de programación R que permite la ejecución de código arbitrario al deserializar datos no confiables. Esta vulnerabilidad puede ser explotada a través de la carga de archivos RDS (Serialización de Datos R) o paquetes R, que a menudo son compartidos entre desarrolladores y científicos de datos. Un atacante puede crear archivos RDS maliciosos o paquetes R que contengan código R arbitrario incrustado que se ejecute en el dispositivo objetivo de la víctima al interactuar con ellos.

Prioridad: 3 Importante.

Ampliar información:

https://www.helpnetsecurity.com/2024/04/29/prompt-fuzzer-open-source-genai-applications-security/

XSS en GitLab: vulnerabilidad de script

El equipo de investigación de amenazas de SonicWall Capture Labs se percató de una vulnerabilidad de script entre sitios (XSS) en GitLab, evaluó su impacto y desarrolló medidas de mitigación. GitLab, una plataforma de intercambio de código abierto, publicó un aviso

sobre esta vulnerabilidad que afecta a GitLab CE/EE en todas las versiones desde la 16.7 hasta la 16.8.6, la 16.9 antes de la 16.9.4 y la 16.10 antes de la 16.10.2. Identificada como CVE-2024-2279, permite que actores de amenazas remotos realicen acciones arbitrarias en nombre de las víctimas, obteniendo una alta puntuación de CVSS de 8.7.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.sonicwall.com/en-us/2024/04/gitlab-xss-via-autocomplete-results/

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

El nuevo botnet "Goldoon"

Se ha observado un nuevo botnet llamado “Goldoon”, que tiene como objetivo los routers D-Link con una vulnerabilidad crítica con casi una década de antigüedad, su objetivo es utilizar los dispositivos comprometidos para realizar más ataques. La vulnerabilidad en cuestión es CVE-2015-2051 (puntuación CVSS: 9.8), que afecta a los routers D-Link DIR-645 y permite a atacantes remotos ejecutar comandos arbitrarios mediante solicitudes HTTP especialmente diseñadas. 'Si un dispositivo específico es comprometido, los atacantes pueden obtener control completo, lo que les permite extraer información del sistema, establecer comunicación con un servidor C2 y luego usar estos dispositivos para lanzar ataques adicionales, como ataques de denegación de servicio distribuido (DDoS)', dijeron los investigadores de Fortinet FortiGuard Labs, Cara Lin y Vincent Li.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/05/new-goldoon-botnet-targets-d-link.html

---

Ciberdelincuentes y Estados-Nación compartiendo redes comprometidas

Los ciberdelincuentes y los actores de Amenazas Persistentes Avanzadas (APT) comparten un interés común en capas de anonimización de proxy y nodos de Red Privada Virtual (VPN) para ocultar rastros de su presencia y dificultar la detección de actividades maliciosas. Este interés compartido da como resultado que el tráfico de internet malicioso mezcle motivos financieros y de espionaje.

Prioridad: 3 Importante.

Ampliar información:

https://www.trendmicro.com/en_us/research/24/e/router-roulette.html

---

Suplantación de identidad en Shein para recolección de credenciales

Shein es una de las aplicaciones de compras más populares del mundo. De hecho, es la segunda aplicación de compras más descargada a nivel mundial, con más de 251 millones de descargas. La plataforma de comercio electrónico es buscada con más frecuencia en Google que marcas importantes como Nike y Adidas. Shein ganó popularidad por su ropa económica y precios bajos. Sin embargo, la empresa ha enfrentado críticas significativas por su pobre historial en derechos humanos.

Prioridad: 3 importante.

Ampliar información:

https://blog.checkpoint.com/harmony-email/spoofing-shein-for-credential-harvesting/

Troyano de acceso remoto para Android equipado para recolectar credenciales

El equipo de investigación de amenazas de SonicWall Capture Labs ha estado compartiendo regularmente información sobre malware dirigido a dispositivos Android. Se han encontrado muestras de RAT similares antes, pero esta incluye comandos adicionales y ataques de phishing diseñados para recolectar credenciales.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.sonicwall.com/en-us/2024/04/android-remote-access-trojan-equipped-to-harvest-credentials/

Zero-Day del 2017 más Carga de Cobalt Strike en una alianza inmoral

El Laboratorio de Amenazas de Deep Instinct observó un archivo PPSX malicioso cargado desde Ucrania a VirusTotal a finales de 2023. El nombre del archivo sugiere que fue compartido a través de la aplicación Signal; sin embargo, esto no significa que el archivo haya sido enviado inicialmente a la víctima a través de la aplicación.

Prioridad: 2 Urgente.

Ampliar información:

https://www.hackread.com/microsoft-office-0-day-exploited-cobalt-strike/

El malware ZLoader evoluciona con anti-análisis del troyano bancario Zeus

Los autores detrás del resurgimiento del malware ZLoader han añadido una característica que estaba originalmente presente en el troyano bancario Zeus, del cual se basa, lo que indica que está siendo desarrollado activamente. "La última versión, 2.4.1.0, introduce una característica para evitar la ejecución en máquinas que difieren de la infección original", dijo el investigador de Zscaler ThreatLabz, Santiago Vicente, en un informe técnico. "Una característica similar de anti-análisis estaba presente en el código fuente filtrado de ZeuS 2.X, pero implementado de manera diferente."

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/04/us-government-releases-new-ai-security.html

---

Nuevos ataques de malware Latrodectus utilizan temas de Microsoft y Cloudflare

El malware Latrodectus ahora se está distribuyendo en campañas de phishing utilizando señuelos de Microsoft Azure y Cloudflare para aparecer legítimo mientras dificulta que las plataformas de seguridad de correo electrónico detecten los correos electrónicos como maliciosos. Latrodectus (también conocido como Unidentified 111 e IceNova) es un malware descargador de Windows, descubierto por primera vez por el equipo de seguridad de Walmart y luego analizado por ProofPoint y Team Cymru, que actúa como una puerta trasera, descargando cargas útiles adicionales de EXE y DLL o ejecutando comandos.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/new-latrodectus-malware-attacks-use-microsoft-cloudflare-themes/

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

¿Por qué las vulnerabilidades en la nube necesitan CVEs?

Al considerar el propósito de la gestión de vulnerabilidades en un mundo moderno, es imperativo reconocer la gran transición hacia nuevas tecnologías y cómo se maneja el riesgo dentro de estos diferentes paradigmas y entornos (por ejemplo, la nube). Parchar la seguridad de la red no es aplicable de la misma manera para los entornos en la nube, y pocos proveedores de servicios en la nube asignan identificadores de Exposiciones y Vulnerabilidades Comunes (CVE) a las vulnerabilidades.

Prioridad: 3 Importante.

Ampliar información:

https://www.helpnetsecurity.com/2024/05/01/cve-vulnerability-management/

Change Healthcare fue hackeado utilizando una cuenta de Citrix robada

UnitedHealth confirma que la red de Change Healthcare fue comprometida por la banda de ransomware BlackCat, quienes utilizaron credenciales robadas para iniciar sesión en el servicio de acceso remoto de Citrix de la compañía, el cual no tenía habilitada la autenticación multifactor. Esto fue revelado en el testimonio por escrito del CEO de

UnitedHealth, Andrew Witty, publicado antes de una audiencia del subcomité de la Cámara de Energía y Comercio programada para mañana.

Prioridad: 3 Importante.

Ampliar información:

https://www.itnews.com.au/news/unitedhealth-hackers-used-citrix-vulnerability-to-break-in-607552

LockBit, Black Basta y Play dominan el panorama del ransomware en el primer trimestre de 2024

LockBit, Black Basta y Play han sido observados como los grupos de ransomware más activos en el primer trimestre de 2024, con Black Basta experimentando un notable aumento del 41% en su actividad. Los datos provienen del último informe de la firma de ciberseguridad ReliaQuest, que también sugiere que durante el mismo período, LockBit enfrentó un importante revés debido a acciones de las fuerzas del orden en febrero. A pesar de los esfuerzos por restaurar las operaciones, la actividad de LockBit disminuyó un 21% en comparación con el trimestre anterior. La reputación del grupo entre los afiliados también sufrió, con conversaciones en los foros de ciberdelincuentes reflejando aprehensión sobre colaborar con un grupo comprometido por las fuerzas del orden. Mientras tanto, la aparición del grupo DarkVault sugiere una posible estrategia de cambio de marca por parte de LockBit.

Prioridad: 3 Importante.

Ampliar información:

https://www.infosecurity-magazine.com/news/lockbit-black-basta-playl

---

Las herramientas de escritorio remoto más atacadas en el último año

El software de escritorio remoto permite a los empleados conectarse a su red informática sin estar físicamente vinculados al dispositivo principal o incluso en la misma ubicación. Esto lo convierte en una herramienta útil para una fuerza laboral distribuida o remota. Desafortunadamente, el software de escritorio remoto también es un objetivo principal para los ciberataques.

Prioridad: 3 Importante.

Ampliar información:

https://blog.barracuda.com/2024/05/01/threat-spotlight-remote-desktop-tools-most-targeted