GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

En alianza con

TD SYNNEX FORTINET

Edición °3624

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	2	1	0
MALWARE	1	2	1
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

Vulnerabilidad crítica en WPML expone sitios de WordPress a ejecución remota de código

Una vulnerabilidad crítica en el plugin WPML para WordPress, identificada como CVE-2024-6386 (CVSS: 9.9), permite a usuarios autenticados con permisos de Colaborador o superiores ejecutar código de forma remota en el servidor. Este fallo, presente en versiones anteriores a la 4.6.13, surge por la falta de validación y saneamiento de entradas, lo que habilita inyecciones de plantillas del lado del servidor (SSTI). Se recomienda a los usuarios actualizar el plugin para mitigar posibles amenazas.

Prioridad: 1 Crítico.

Ampliar información:

https://thehackernews.com/2024/08/critical-wpml-plugin-flaw-exposes.html

---

Vulnerabilidad crítica en Apache OFBiz bajo explotación activa

La vulnerabilidad CVE-2024-38856 (CVSS: 9.8) en Apache OFBiz está siendo explotada activamente, permitiendo la ejecución remota de código mediante un payload Groovy en el contexto del usuario OFBiz, sin necesidad de autenticación. Se recomienda a las organizaciones actualizar a la versión 18.12.15 para mitigar el riesgo.

Prioridad: 1 Crítico.

Ampliar información:

https://thehackernews.com/2024/08/cisa-flags-critical-apache-ofbiz-flaw.html

---

Cisco corrige múltiples vulnerabilidades en el software NX-OS

El 29 de agosto de 2024, Cisco lanzó actualizaciones para su software NX-OS, abordando diversas vulnerabilidades, entre ellas una falla crítica de Denegación de Servicio (DoS) identificada como CVE-2024-20446. Esta vulnerabilidad en el agente de retransmisión DHCPv6 podría ser explotada por atacantes remotos no autenticados para causar un reinicio repetido del dispositivo afectado, lo que resultaría en una condición de DoS. Además, las actualizaciones incluyen correcciones para fallas de inyección de comandos y problemas de escape de sandbox en el intérprete de Python.

Prioridad: 2 Urgente.

Ampliar información:

https://www.securityweek.com/cisco-patches-multiple-nx-os-software-vulnerabilities/

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

Mirai aprovecha Zero-Day de hace 5 años para infectar cámaras IP

La variante Corona de la botnet Mirai está utilizando una vulnerabilidad de Ejecución Remota de Código (CVE-2024-7029) en cámaras IP AVTECH, explotando un fallo en el ajuste de brillo del firmware que permite a atacantes no autenticados inyectar comandos. Este exploit afecta a modelos descontinuados que ya no reciben soporte, dejando a los dispositivos expuestos sin solución. Se recomienda desconectar y reemplazar las cámaras afectadas para mitigar el riesgo de ataques DDoS y otras amenazas.

Prioridad: 3 Importante.

Ampliar información:

https://blog.segu-info.com.ar/2024/08/malware-mirai-aprovecha-zero-day-de.html

---

Malware disfrazado de Palo Alto GlobalProtect instala puertas traseras en empresas

Actores maliciosos están utilizando una versión falsa del software Palo Alto GlobalProtect para atacar organizaciones, con el objetivo de robar datos y ejecutar comandos remotos de PowerShell. Esta campaña, descubierta por Trend Micro, se inicia a través de un archivo malicioso que simula ser el instalador de GlobalProtect, pero que en realidad carga malware en segundo plano, permitiendo a los atacantes infiltrarse en las redes internas de las empresas.

Prioridad: 1 Crítico.

Ampliar información:

https://www.bleepingcomputer.com/news/security/fake-palo-alto-globalprotect-used-as-lure-to-backdoor-enterprises/?&web_view=true

---

Nueva variante de ransomware Cicada3301 ataca sistemas VMware ESXi

Una nueva operación de ransomware conocida como Cicada3301 ha surgido en el panorama de amenazas, apuntando a empresas con un enfoque particular en sistemas VMware ESXi. Este ransomware, escrito en Rust, muestra similitudes con el grupo ALPHV, incluyendo el uso de ChaCha20 para la encriptación y comandos similares para gestionar máquinas virtuales. La campaña Cicada3301, activa desde junio, se caracteriza por su

capacidad de operar tanto en entornos Windows como Linux/ESXi, sugiriendo una posible conexión o evolución del grupo ALPHV.

Prioridad: 2 Urgente.

Ampliar información:

https://securityaffairs.com/167897/cyber-crime/a-new-variant-of-cicada-ransomware-targets-vmware-esxi-systems.html?web_view=true

---

Ataques con Lumma Stealer se expanden a través de comentarios en GitHub

El 30 de agosto de 2024, se reportó que cibercriminales están utilizando plataformas como GitHub para diseminar el malware Lumma Stealer, un avanzado ladrón de información diseñado para robar contraseñas almacenadas, cookies, datos de criptomonedas e información de clientes de correo electrónico. Este malware, ofrecido a través de un modelo de Malware-as-a-Service (MaaS), se distribuye en comentarios en repositorios públicos de GitHub que contienen enlaces a archivos cifrados en mediafire[.]com, con contraseñas genéricas como "changeme". Aunque GitHub está trabajando en la eliminación de estos comentarios maliciosos, la rapidez con la que se generan nuevos posts dificulta la tarea. Además de GitHub, se han observado campañas similares en YouTube, donde Lumma Stealer se presenta bajo la apariencia de "Tutoriales falsos", engañando a los usuarios con promesas de software gratuito.

Prioridad: 2 Urgente.

Ampliar información:

https://gbhackers.com/lumma-stealer-malware-github/

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

RansomHub Ransomware Afecta 210 Víctimas en Sectores Críticos

Desde febrero de 2024, el grupo RansomHub ha cifrado y exfiltrado datos de al menos 210 víctimas en sectores críticos como salud, servicios gubernamentales y tecnología. Este ransomware-as-a-service, una evolución de Cyclops y Knight, utiliza un modelo de doble extorsión y ha aumentado significativamente su actividad, representando el 14.2% de todos los ataques en el tercer trimestre de 2024. Los ataques se facilitan mediante la explotación de vulnerabilidades en diversos sistemas y la exfiltración de datos a través de métodos sofisticados.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/09/ransomhub-ransomware-group-targets-210.html

---