GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

En alianza con

TD SYNNEX FORTINET

Edición °4024

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
VULNERABILIDADES	3	0	0
MALWARE	0	1	1
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

HPE Aruba corrige vulnerabilidades críticas de RCE en puntos de acceso

HPE Aruba Networking solucionó tres vulnerabilidades críticas de ejecución remota de código (RCE) en sus puntos de acceso. Las fallas, identificadas como CVE-2024-42505, CVE-2024-42506, y CVE-2024-42507, permiten a atacantes no autenticados enviar paquetes maliciosos al puerto UDP 8211 del Protocolo de Administración de Puntos de Acceso (PAPI) para ejecutar código arbitrario.

Se recomienda actualizar a las versiones corregidas de AOS-8 y AOS-10 para mitigar el riesgo, o bloquear el puerto en redes no confiables como solución temporal. No se han detectado explotaciones activas hasta la fecha.

Prioridad: 1 Crítico.

Ampliar información:

https://www.bleepingcomputer.com/news/security/hpe-aruba-networking-fixes-three-critical-rce-flaws-impacting-its-access-points/

Crítica vulnerabilidad en Ivanti vTM explotada activamente

Recientemente, se ha detectado la explotación activa de la vulnerabilidad de omisión de autenticación en Ivanti Virtual Traffic Manager (vTM), identificada como CVE-2024-7593 con un puntaje CVSS de 9.8. Este fallo permite a atacantes remotos no autenticados evadir las medidas de seguridad del panel de administración y crear cuentas de administrador maliciosas. La vulnerabilidad afecta a versiones anteriores de vTM antes de 22.2R1, 22.3R3, 22.5R2, 22.6R2 y 22.7R2, y está siendo activamente explotada, lo que ha llevado a la Agencia de Seguridad Cibernética e Infraestructura (CISA) a incluirla en su catálogo de vulnerabilidades conocidas y explotadas.

Como recomendación, Ivanti ha lanzado parches para las versiones afectadas y ha instado a los administradores a actualizar sus sistemas de inmediato. También se aconseja restringir el acceso al panel de administración únicamente a redes internas o privadas y revisar los registros de auditoría para detectar posibles signos de explotación, como la creación no autorizada de cuentas de administrador

Prioridad: 1 Crítico.

Ampliar información:

https://www.bleepingcomputer.com/news/security/critical-ivanti-vtm-auth-bypass-bug-now-exploited-in-attacks/

Vulnerabilidad Crítica en NVIDIA Container Toolkit expone sistemas a ataques

Una vulnerabilidad crítica, CVE-2024-0132, afecta al *NVIDIA Container Toolkit* en versiones hasta la 1.16.1, permitiendo a atacantes escapar de contenedores y obtener acceso completo al sistema host. Este fallo es de tipo *Time-of-Check Time-of-Use* (TOCTOU), se puede explotar mediante la ejecución de una imagen de contenedor maliciosa, que aprovecha permisos no seguros para interactuar con el sistema anfitrión.

NVIDIA lanzó parches el 26 de septiembre de 2024, corrigiendo el problema en la versión 1.16.2 del *Container Toolkit* y la 24.6.2 del *GPU Operator*. Se recomienda encarecidamente a los administradores actualizar estas herramientas y evitar el uso de imágenes de contenedor no confiables para mitigar riesgos de ataque. Dado que más del 35% de las aplicaciones en la nube utilizan este toolkit, la explotación de esta vulnerabilidad podría desencadenar incidentes graves, comprometiendo no solo los sistemas afectados, sino también otros contenedores que compartan recursos GPU en la misma infraestructura

Prioridad: 1 Crítico.

Ampliar información:

https://thehackernews.com/2024/09/critical-nvidia-container-toolkit.html

---

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

Hackers usan IA para crear malware en ataques dirigidos

Un grupo de cibercriminales está utilizando inteligencia artificial generativa para desarrollar malware, específicamente el AsyncRAT, en campañas dirigidas a usuarios franceses. HP Wolf Security identificó este malware, distribuido mediante un archivo ZIP protegido por contraseña, oculto en correos electrónicos de phishing. El código fue escrito y comentado de una forma que sugiere el uso de IA. Este malware es capaz de registrar teclas, permitir acceso remoto y desplegar cargas adicionales.

Se recomienda mejorar la detección y prevención de phishing, usar autenticación multifactor (MFA) y limitar el acceso a recursos críticos para mitigar estos ataques basados en IA.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/hackers-deploy-ai-written-malware-in-targeted-attacks/

Nueva Campaña de HTML Smuggling Distribuye DCRat

Investigadores de Netskope han identificado una campaña de *HTML Smuggling* que entrega el troyano DCRat a usuarios de habla rusa. Este método inserta un archivo HTML malicioso que, al abrirse en el navegador de la víctima, descarga un archivo ZIP protegido por contraseña que contiene el malware. DCRat, activo desde 2018, permite ejecutar comandos remotos, registrar teclas y robar credenciales. Para mitigar el riesgo, se recomienda monitorear el tráfico HTTP/HTTPS y evitar la apertura de archivos de fuentes no confiables.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/09/new-html-smuggling-campaign-delivers.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

Microsoft identifica al grupo Storm-0501 como amenaza importante en ataques a la nube híbrida

Microsoft ha identificado a "Storm-0501", un grupo cibercriminal con motivaciones financieras, como un actor clave en ataques dirigidos a infraestructuras de nube híbrida. Este grupo ha utilizado ransomware y técnicas de acceso inicial contra industrias gubernamentales y manufactureras. Se ha enfocado en vulnerabilidades dentro de herramientas críticas, como Zoho ManageEngine y Citrix NetScaler.
Microsoft recomienda implementar autenticación multifactor (MFA), mantener actualizadas las aplicaciones vulnerables, además de reducir los privilegios administrativos para mitigar estos ataques. También, sugiere monitorear actividades sospechosas y aplicar parches de seguridad rápidamente para evitar la explotación de vulnerabilidades.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/09/microsoft-identifies-storm-0501-as.html

Vulnerabilidad crítica en vehículos Kia permitió control remoto

Investigadores de ciberseguridad, liderados por Sam Curry, descubrieron en junio de 2024 vulnerabilidades críticas en el portal de concesionarios de Kia que permitían a los atacantes controlar remotamente vehículos usando solo la matrícula. Estos ataques podían ejecutarse en 30 segundos, afectando a modelos desde 2013 hasta 2025, sin importar si tenían suscripciones activas a Kia Connect. Los atacantes podían desbloquear puertas, arrancar el motor, e incluso acceder a datos personales sensibles como nombre, teléfono y dirección del propietario. Aunque Kia corrigió la vulnerabilidad en agosto, este incidente destaca los riesgos crecientes en los vehículos conectados a internet.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/europol-takes-down-ghost-encrypted-messaging-platform-used-for-crime/
