GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

En alianza con

TD SYNNEX FORTINET

Edición °3324

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

VULNERABILIDADES

Vulnerabilidad en 5G permitió espionaje en teléfonos móviles

Investigadores de la Universidad Estatal de Pensilvania descubrieron una vulnerabilidad en la red 5G que exponía a los usuarios de teléfonos móviles al espionaje. Los ciberdelincuentes podían utilizar estaciones base falsas para interceptar comunicaciones y robar datos personales. Los hallazgos fueron presentados en Black Hat 2024, revelando que marcas como Samsung, Google y Motorola fueron afectadas. Afortunadamente, los proveedores ya han lanzado parches para corregir el problema.

Prioridad: 3 Importante.

Ampliar información:

https://blog.segu-info.com.ar/2024/08/vulnerabilidades-en-banda-5g-permite.html

---

Cuatro vulnerabilidades críticas en OpenVPN exponen a usuarios a ejecución remota de código

Microsoft ha revelado cuatro vulnerabilidades críticas en OpenVPN 2.x que, si se encadenan, permiten la ejecución remota de código (RCE) y la escalada de privilegios locales (LPE). Las fallas afectan versiones anteriores a 2.6.10 y 2.5.10. Además, se encuentran principalmente en el componente openvpnserv. Los atacantes podrían tomar el control total de los sistemas vulnerables si obtienen credenciales de OpenVPN. Aunque requieren autenticación, estas vulnerabilidades representan un riesgo significativo para la seguridad de los sistemas afectados.

Prioridad: 1 Crítico.

Ampliar información:

https://blog.segu-info.com.ar/2024/08/cuatro-vulnerabilidades-criticas-en.html

---

Vulnerabilidades en MongoDB permiten la escalada de privilegios

MongoDB ha divulgado una vulnerabilidad crítica, CVE-2024-7553, que permite la escalada de privilegios en sistemas con versiones específicas de MongoDB Server, C Driver y PHP Driver. La falla, originada por una validación incorrecta de archivos desde directorios no confiables, afecta principalmente a sistemas Windows. Con un puntaje CVSS de 7.3, esta vulnerabilidad es de alta severidad y puede ser explotada localmente con bajo esfuerzo. Se recomienda actualizar a las versiones más recientes de los productos afectados para mitigar el riesgo.

Prioridad: 2 Urgente.

Ampliar información:

https://gbhackers.com/mongodb-vulnerabilities

Ewon Cosy+ expuesto a ataques de acceso root en herramienta de acceso remoto industrial

Se han revelado vulnerabilidades críticas en la herramienta de acceso remoto industrial Ewon Cosy+, que podrían permitir a los atacantes obtener acceso root a los dispositivos. Este acceso elevado podría ser utilizado para descifrar archivos de firmware y datos cifrados, como contraseñas en archivos de configuración, obteniendo certificados VPN X.509 firmados correctamente para tomar el control de sesiones VPN ajenas. Un atacante podría aprovechar una vulnerabilidad de inyección de comandos del sistema operativo, una elusión de filtros, más una vulnerabilidad de XSS persistente para obtener acceso administrativo y root. Además, los atacantes podrían secuestrar sesiones VPN, realizar ataques adicionales accediendo a servicios de red del cliente afectado.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/08/industrial-remote-access-tool-ewon-cosy.html

---

AWS corrige vulnerabilidades críticas que podrían permitir la toma de control de cuentas

AWS ha corregido vulnerabilidades en varios productos, incluidas fallas que podrían haber permitido la toma de control de cuentas. Las debilidades fueron descubiertas por Aqua Security y se revelaron en la conferencia Black Hat USA 2024. Las fallas afectaban servicios como CloudFormation, Glue, EMR, SageMaker, ServiceCatalog y CodeStar, y podrían haber llevado a la ejecución de código arbitrario, exposición de datos sensibles, ataques de denegación de servicio y manipulación de modelos de IA. Los investigadores demostraron

cómo los atacantes podían aprovechar nombres predecibles de buckets en S3 para almacenar código malicioso y obtener privilegios elevados. AWS ha confirmado que las vulnerabilidades han sido solucionadas.

Prioridad: 3 Importante.

Ampliar información:

https://www.securityweek.com/aws-patches-vulnerabilities-potentially-allowing-account-takeovers//

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 DeerStealer se distribuye como Google Authenticator falso

Investigadores de ANY.RUN han descubierto un nuevo malware llamado DeerStealer, que se distribuye a través de sitios web falsos que imitan la página oficial de Google. La campaña, activa desde julio, engaña a los usuarios para que descarguen una versión falsa de Google Authenticator. El malware extrae datos sensibles del dispositivo infectado, como información del navegador y FTP, y se comunica con un servidor C2 similar al del malware XFiles, aunque reescrito en otro lenguaje.

Prioridad: 3 Importante.

Ampliar información:

https://blog.segu-info.com.ar/2024/08/nuevo-malware-deerstealer-distribuido.html

---

Ransomware BlackSuit Causa Estragos en América Latina

El ransomware BlackSuit, anteriormente conocido como Royal, ha estado activo en América Latina, exigiendo rescates de hasta 500 millones de dólares. Los atacantes negocian los montos a través de la red To, dirigiendo sus ataques a sectores críticos como salud y manufactura. BlackSuit desactiva antivirus, luego exfiltra datos antes de cifrar sistemas. Utilizan tácticas agresivas como amenazas directas a víctimas secundarias para aumentar la presión. Este ataque se suma a la creciente evolución de familias de ransomware, que siguen perfeccionando sus métodos y herramientas.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.segu-info.com.ar/2024/08/ransomware-blacksuit-ex-royal-activo-en.html

---

Grupo Ransomware Hunters International ataca redes corporativas con SharpRhino RAT

El grupo de ransomware Hunters International, conocido por su similitud de código con la peligrosa banda Hive, ha comenzado a atacar redes corporativas utilizando el troyano de acceso remoto SharpRhino (RAT). Este malware se disfraza como el instalador de Angry IP Scanner, una herramienta utilizada por profesionales de TI. SharpRhino modifica el registro de Windows, crea accesos directos maliciosos y ejecuta scripts de PowerShell para mantener su presencia en el sistema. Para protegerse, se recomienda utilizar filtrado DNS avanzado, segmentación de red y políticas de cero confianza para evitar la propagación de infecciones.

Prioridad: 3 Importante.

Ampliar información:

https://heimdalsecurity.com/blog/raas-sharprhino-rat/

Campaña de malware afecta a 300,000 usuarios con extensiones falsas para Chrome y Edge

Una extensa campaña de malware ha infectado a al menos 300,000 usuarios de Google Chrome y Microsoft Edge mediante la instalación de extensiones fraudulentas. El malware se distribuye a través de trojans disfrazados de descargas populares en sitios web falsos, que promueven programas como Roblox FPS Unlocker o VLC Media Player. Estas

extensiones maliciosas, imposibles de desactivar incluso en el modo de desarrollador, redirigen búsquedas a servidores controlados por los atacantes, ejecutan comandos que interceptan y manipulan el tráfico web. Se recomienda a los afectados eliminar tareas programadas, claves del registro o archivos asociados para mitigar el daño.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/08/new-malware-hits-300000-users-with.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

Mejores Prácticas para Optimizar el Uso de EDR en 2024

En 2024, es crucial para las empresas optimizar sus soluciones de EDR (Detección y Respuesta de Endpoints) para mejorar la detección y respuesta a amenazas cibernéticas. Las mejores prácticas incluyen identificar los mayores riesgos, implementar una seguridad en capas, evitar la superposición de múltiples herramientas, desplegar las políticas gradualmente, automatizar respuestas cuando sea posible, reducir falsos positivos, as+i como ajustar las políticas basadas en monitoreo constante. Utilizar una plataforma XDR moderna que integre todas estas funciones es esencial para una protección más eficiente y efectiva.

Prioridad: 3 Importante.

Ampliar información:

https://heimdalsecurity.com/blog/edr-best-practices/

Actores maliciosos aprovechan servicios en la nube para operaciones de ciberespionaje

En el último año, se ha observado un incremento en el uso de servicios legítimos en la nube por parte de actores maliciosos, incluidos grupos respaldados por estados. Estos atacantes utilizan servicios confiables como Microsoft OneDrive y Google Drive para evitar la detección, empleando herramientas como el troyano GoGra, que interactúa con servidores de comando y control a través de la API de Microsoft Graph. Las operaciones de espionaje, como las de los grupos Harvester y Firefly, han adoptado estas tácticas para infiltrarse en organizaciones de alto perfil.

Prioridad: 2 Urgente.

Ampliar información:

https://symantec-enterprise-blogs.security.com/threat-intelligence/cloud-espionage-attacks

---