GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0225

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

VULNERABILIDADES

Fortinet soluciona múltiples vulnerabilidades de diferentes productos

El día 14 de enero de 2025, Fortinet publicó 52 parches de seguridad para abordar múltiples vulnerabilidades que afectaban a una amplia gama de sus productos. Estas brechas de seguridad, que variaban en severidad desde baja hasta crítica, podrían haber sido explotadas por actores maliciosos para comprometer la seguridad de las redes y los sistemas de las organizaciones que utilizaban estos equipos.

Entre los productos afectados se encontraban los firewalls de próxima generación FortiGate, los servidores web seguros FortiWeb y los servidores de correo electrónico FortiMail. Las vulnerabilidades más críticas podrían haber permitido a atacantes remotos ejecutar código arbitrario en los sistemas afectados, lo que podría haber resultado en la pérdida de datos confidenciales, la interrupción de servicios críticos y, en algunos casos, el control total de los sistemas comprometidos.

Para más información, se recomienda consultar la plataforma de Fortinet, aplicar los filtros adecuados al entorno corporativo y seguir las recomendaciones proporcionadas.

Prioridad: Crítico

Ampliar información:

https://www.fortiguard.com/psirt?filter=1&version=&date=2025

Dell, HPE y MediaTek publican parches para vulnerabilidades críticas

Dell, HPE y MediaTek han lanzado actualizaciones para corregir vulnerabilidades graves en sus productos. MediaTek resolvió una falla crítica (CVE-2024-20154) en el componente de módem de varios chipsets, que permitía la ejecución remota de código al conectarse a estaciones base maliciosas. También abordó siete fallos de alta severidad relacionados con escalación de privilegios y ejecución remota de código. Dell corrigió una vulnerabilidad de alta severidad (CVE-2025-22395) en su DUP Framework, que permitía la ejecución de scripts arbitrarios y condiciones de denegación de servicio (DoS), además de problemas en productos afectados por una falla de Apache Tomcat (CVE-2024-52316). HPE solucionó múltiples fallos en componentes de terceros de sus switches SAN con Brocade Fabric OS, abarcando escalación de privilegios, ejecución remota de comandos y creación o eliminación de archivos. Aunque no se reportan explotaciones activas, los usuarios deben aplicar los parches inmediatamente para mitigar riesgos.

Prioridad: Urgente

Ampliar información:

https://www.securityweek.com/dell-hpe-mediatek-patch-vulnerabilities-in-their-products/

Primera actualización de seguridad de Android 2025 corrige vulnerabilidades críticas

Google lanzó la primera actualización de seguridad de Android para 2025, corrigiendo 36 vulnerabilidades, incluidas cinco de severidad crítica que afectan a las versiones 12, 12L, 13, 14 y 15 del sistema operativo. Estas fallas, identificadas como CVE-2024-43096 y otras, permiten la ejecución remota de código sin privilegios adicionales. La actualización se divide en dos niveles: el 2025-01-01 aborda 24 problemas en los componentes Framework, Media Framework y System, mientras que el 2025-01-05 corrige 12 fallos en tecnologías de MediaTek, Qualcomm e Imagination Technologies. También incluye un parche crítico para dispositivos Pixel (CVE-2024-53842). Aunque no se han reportado explotaciones activas, se insta a los usuarios a actualizar sus dispositivos para mitigar riesgos.

Prioridad: Urgente

Ampliar información:

https://www.securityweek.com/first-android-update-of-2025-patches-critical-code-execution-vulnerabilities/

Actualizaciones de Chrome y Firefox corrigen vulnerabilidades graves

Google y Mozilla lanzaron actualizaciones de seguridad para Chrome 131 y Firefox 134, resolviendo vulnerabilidades de alta gravedad en ambos navegadores. Chrome corrigió cuatro fallos, incluido un defecto de confusión de tipo en el motor V8 (CVE-2025-0291), que podría permitir la ejecución remota de código y otorgó al investigador que lo reportó una recompensa de $55,000. Las versiones actualizadas de Chrome están disponibles para Windows, macOS y Linux. Por su parte, Firefox abordó 11 vulnerabilidades, entre ellas tres graves: dos fallos de seguridad de memoria y un defecto de suplantación en la barra de direcciones en Firefox para Android (CVE-2025-0244). Las actualizaciones incluyen

también Firefox ESR 115.19 y 128.6, enfocadas en problemas similares. Aunque no se han detectado explotaciones activas, se recomienda a los usuarios actualizar sus navegadores de inmediato.

Prioridad: Importante

Ampliar información:

https://www.securityweek.com/chrome-131-firefox-134-updates-patch-high-severity-vulnerabilities/

Palo Alto Networks corrige fallas graves en herramienta de migración retirada

Palo Alto Networks ha corregido varias vulnerabilidades en su herramienta Expedition, retirada a finales de 2024, incluyendo un fallo crítico (CVE-2025-0103) que permite la inyección de SQL, exponiendo datos sensibles como contraseñas, configuraciones de dispositivos y claves de API. Aunque Expedition estaba diseñada como una solución temporal para migrar a su plataforma de firewall NGFW y ya no recibirá actualizaciones, la empresa recomienda restringir su acceso y considerar alternativas. También se corrigieron vulnerabilidades menores relacionadas con divulgación de información y ejecución de JavaScript. Palo Alto Networks instó a los usuarios a aplicar los parches de inmediato para mitigar riesgos.

Prioridad: Urgente

Ampliar información:

https://www.securityweek.com/palo-alto-networks-patches-high-severity-vulnerability-in-retired-migration-tool/

Recomendaciones generales sobre vulnerabilidades:

- Siempre instale los parches más recientes publicados por los fabricantes para corregir vulnerabilidades críticas y mitigar riesgos.
- Limite el acceso a herramientas o servicios no utilizados y restrinja los puertos abiertos solo a usuarios y redes confiables.
- Configure alertas para detectar intentos de acceso inusuales o comportamientos anómalos en servidores y sistemas críticos.
- Realice pruebas de penetración y revisiones de seguridad regulares para identificar vulnerabilidades no reportadas.
- Aplique controles de acceso basados en roles y segmentación de red para minimizar el impacto en caso de una vulnerabilidad explotada.

MALWARE

Nuevo malware NonEuclid RAT aumenta amenaza cibernética global

El malware NonEuclid RAT, un troyano de acceso remoto avanzado diseñado en C#, representa una creciente amenaza cibernética. Este software malicioso, desarrollado para evadir antivirus y cifrar archivos críticos, utiliza técnicas sofisticadas como escalada de privilegios, persistencia mediante manipulación del registro y cargas dinámicas de DLL. Su capacidad para robar credenciales, datos sensibles y carteras de criptomonedas lo convierte en un arma poderosa para ciberdelincuentes. Además, permite el control remoto de sistemas infectados para actividades maliciosas, incluyendo exfiltración de datos y ataques de botnets. Popularizado en foros rusos y campañas de phishing, su impacto global exige refuerzos en la inteligencia de amenazas y medidas de ciberseguridad proactivas.

Prioridad: Urgente

Ampliar información:

https://gbhackers.com/noneuclid-rat-antivirus-bypass/

Malware Banshee para macOS amplía su alcance global

El malware Banshee, diseñado para robar información en sistemas macOS, ha eliminado su restricción de idioma ruso, expandiendo su objetivo a nivel global. Inicialmente detectado en 2024 y ofrecido en foros de ciberdelincuencia por $3,000 al mes, Banshee recopila contraseñas, información del sistema, datos de navegadores y carteras de criptomonedas. Tras la filtración de su código fuente en noviembre de 2024, las detecciones antivirus mejoraron, pero también surgieron preocupaciones por posibles variantes desarrolladas por otros actores. Actualmente, el malware sigue distribuyéndose a través de sitios de phishing y repositorios falsos en GitHub. Check Point reporta múltiples campañas activas y advierte sobre su creciente sofisticación y alcance.

Prioridad: Crítico

Ampliar información:

https://www.securityweek.com/banshee-macos-malware-expands-target-list/

Recomendaciones generales sobre malware:

- Mantenga siempre actualizados los sistemas antivirus, firewalls y herramientas de detección de amenazas.
- No descargue software ni abra enlaces de correos o sitios web desconocidos. Fomente el uso exclusivo de repositorios oficiales.
- Eduque a los empleados sobre cómo identificar intentos de phishing y engaños en línea.
- Limite los privilegios de usuario y evite que el software descargado sin autorización se ejecute en sistemas corporativos.

- Monitoree el tráfico de red para detectar actividades sospechosas, como conexiones a servidores remotos desconocidos.

NOTICIAS DE CIBERSEGURIDAD

Hackers usan enlaces de YouTube y temas de Microsoft 365 para robar credenciales

Ciberdelincuentes están utilizando tácticas de phishing avanzadas para robar credenciales de usuarios de Microsoft 365, aprovechando URLs engañosas que imitan dominios legítimos. Mediante ingeniería social, crean un falso sentido de urgencia, como avisos de expiración de contraseñas, para inducir a las víctimas a hacer clic en enlaces maliciosos. Estos redirigen a páginas fraudulentas donde se solicitan las credenciales, permitiendo el acceso no autorizado a datos corporativos sensibles. Los atacantes usan prefijos aparentes como "youtube.com" combinados con caracteres de ofuscación (%20 o "@") para ocultar el destino real del enlace, engañando a los usuarios. Para mitigar este riesgo, se recomienda inspeccionar cuidadosamente URLs sospechosas, implementar herramientas de filtrado de enlaces y capacitar a los usuarios en prácticas seguras de correo electrónico.

Prioridad: Urgente

Ampliar información:

https://gbhackers.com/youtube-microsoft-phishing/

RedCurl APT explota tareas programadas de Windows para espionaje cibernético

El grupo APT RedCurl ha sido identificado utilizando tareas programadas en Windows para desplegar malware que ejecuta scripts maliciosos y herramientas como RPivot para conectarse a servidores remotos. Su objetivo principal es la exfiltración de datos hacia almacenamiento en la nube, afectando múltiples industrias y manteniendo persistencia a largo plazo. Emplean técnicas de ofuscación con PowerShell, Python y herramientas nativas como 7zip para ocultar sus actividades. Además, el uso de estrategias "Living-Off-The-Land" dificulta su detección al simular tareas legítimas del sistema. Los analistas de seguridad recomiendan monitoreo continuo, caza de amenazas y defensas en capas para identificar anomalías y proteger datos sensibles frente a estos sofisticados ataques.

Prioridad: Urgente

Ampliar información:

https://gbhackers.com/redcurl-apt-hackers-absuing-windows/

Problemas de MFA en Microsoft 365 impactan el acceso de usuarios

Microsoft ha alertado sobre un problema con la autenticación multifactor (MFA) que está afectando el acceso a aplicaciones de Microsoft 365, como Outlook, Teams y SharePoint. Este incidente, identificado como OP978247, está causando interrupciones para usuarios y empresas que dependen de estos servicios para operaciones diarias. Aunque Microsoft ha implementado redirecciones de tráfico para mitigar el impacto, algunos usuarios aún experimentan bloqueos en el acceso debido a fallos en el paso crítico de autenticación. La compañía continúa investigando y mejorando la disponibilidad del servicio, mientras recomienda a los administradores monitorear las actualizaciones en el centro de administración de Microsoft 365.

Prioridad: Importante

Ampliar información:

https://gbhackers.com/microsoft-warns-of-mfa-issue/

Ataque de Ransomware en Casio expone datos de miles de personas

Casio concluyó su investigación sobre un ataque de ransomware ocurrido en octubre de 2024, confirmando que datos personales y documentos internos fueron comprometidos. Los ciberdelincuentes accedieron a la red mediante vulnerabilidades en oficinas internacionales y correos de phishing. Cerca de 6,500 empleados, 1,900 socios comerciales y 91 clientes fueron afectados. Los datos expuestos incluyen nombres, correos electrónicos, fechas de nacimiento y otra información confidencial, aunque no se encontraron evidencias de robo en bases de datos de clientes ni información de tarjetas de pago. El grupo de ransomware Underground, que reclama la autoría, aseguró haber filtrado más de 200 GB de datos en su sitio de la red Tor. Casio instó a los afectados a reforzar medidas de seguridad y continúa investigando el impacto del ataque.

Prioridad: Importante

Ampliar información:

https://www.securityweek.com/thousands-impacted-by-casio-data-breach/