GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °2423

En alianza con

TD SYNNEX FORTINET

BOLETIN DE CIBERINTELIGENCIA DE AMENAZAS

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	7	1	
MALWARE	1	2	
BRECHAS DE SEGURIDAD		1	
NOTICIAS DE CIBERSEGURIDAD	1	1	
SECTOR FINANCIERO	1		
NOTICIA EN COLOMBIA		1	

VULNERABILIDADES

Fortinet soluciona falla crítica de RCE en SSL VPN (CVE-2023-27997 - XORtigate)

Fortinet ha lanzado nuevas actualizaciones de firmware de Fortigate que corrigen una vulnerabilidad crítica no revelada de ejecución remota de código de autenticación previa en dispositivos SSL VPN. Esta vulnerabilidad crítica en los firewall de Fortinet que afecta a la funcionalidad de SSL-VPN CVE-2023-27997. Se ha apodado "XORtigate". Las correcciones de seguridad se publicaron el viernes de la semana pasada en las versiones de firmware de FortiOS 6.0.17, 6.2.15, 6.4.13, 7.0.12 y 7.2.5.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign
- https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-rce-flaw-in-fortigate-ssl-vpn-devices-patch-now/
- https://www.fortiguard.com/psirt/FG-IR-23-097

Se insta a las organizaciones a abordar vulnerabilidades críticas, detectadas en el primer semestre de 2023

Un reciente informe de Rezilion ha arrojado luz sobre algunas vulnerabilidades notables encontradas en la primera mitad de 2023 y ha proporcionado estrategias de remediación recomendadas. Las vulnerabilidades abarcan diversas fuentes, incluidos los procesos de desarrollo, el software de código abierto y las cadenas de suministro.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.rezilion.com/blog/which-critical-vulnerabilities-discovered-in-2023-can-do-serious-damage-read-our-report/

Exploit para vulnerabilidad de escalamiento de privilegios en Windows

Los investigadores han lanzado un exploit de prueba de concepto (PoC) para una vulnerabilidad de escalamiento de privilegios local de Windows, explotada activamente como parte de los parches de mayo de 2023. El subsistema *Win32k* (controlador de *kernel Win32k.sys*) administra el administrador de ventanas, la salida de pantalla, la entrada y los gráficos del sistema operativo, y actúa como una interfaz entre varios tipos de hardware de entrada. Como tal, explotar este tipo de vulnerabilidades tiende a proporcionar privilegios elevados o ejecución de código.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.numencyber.com/cve-2023-29336-win32k-analysis/ Análisis y PoC (Prueba de Concepto)
- https://www.bleepingcomputer.com/news/security/poc-released-for-windows-win32k-bug-exploited-in-attacks/

Ciberdelincuentes chinos explotan vulnerabilidad Zero-day de VMware en sistemas Windows y Linux

El grupo de ciberdelincuentes UNC3886, patrocinado por China, está llevando a cabo ataques activos utilizando una vulnerabilidad Zero-day en los hosts de VMware ESXi. El objetivo de estos ataques es infiltrar puertas traseras en sistemas operativos Windows y Linux.

La vulnerabilidad de autenticación en VMware Tools, identificada como **CVE-2023-20867** (con una puntuación CVSS: 3.9), permite la ejecución de comandos con privilegios en sistemas operativos Windows, Linux y PhotonOS (vCenter) sin necesidad de

autenticación de credenciales en los sistemas operativos invitados. Esto se logra desde un host ESXi comprometido y sin registro predeterminado en los sistemas operativos invitados.

Prioridad: 2 Urgente.

Ampliar información:

- https://unaaldia.hispasec.com/2023/06/ciberdelincuentes-chinos-explotan-vulnerabilidad-zero-day-de-vmware-en-sistemas-windows-y-linux.html
- https://thehackernews.com/2023/06/chinese-hackers-exploit-vmware-zero-day.html
- https://www.vmware.com/security/advisories/VMSA-2023-0013.html
- https://www.ciberseguridadlatam.com/2023/06/15/delincuentes-chinos-aprovechan-un-dia-cero-de-vmware-para-abrir-puertas-traseras-en-sistemas-windows-y-linux/
- https://blog.segu-info.com.ar/2023/06/zero-day-en-vmare-permite-instalar.html

---

VMware corrige fallas críticas en Aria Operations for Networks (CVE-2023-20887)

VMware solucionó dos vulnerabilidades críticas (**CVE-2023-20887, CVE-2023-20888**) y una importante (**CVE-2023-20889**) en Aria Operations for Networks (anteriormente vRealize Network Insight), su popular herramienta de monitoreo de redes empresariales.

Prioridad: 1 Crítico.

Ampliar información:

- https://github.com/sinsinology/CVE-2023-20887 PoC (Prueba de Concepto)
- https://www.helpnetsecurity.com/2023/06/15/cve-2023-20887-poc-exploit/
- https://www.vmware.com/security/advisories/VMSA-2023-0012.html

Progress Software publica avisos de seguridad para vulnerabilidades de transferencia de MOVEit

Progress Software ha publicado un aviso de seguridad para una vulnerabilidad de escalada de privilegios (**CVE-2023-35708**) en MOVEit Transfer, un software de transferencia de archivos gestionados. Un actor de amenazas cibernéticas podría explotar esta vulnerabilidad para tomar el control de un sistema afectado.

Prioridad: 1 Crítico.

Ampliar información:

- https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023
- https://www.helpnetsecurity.com/2023/06/12/moveit-patch-again/
- https://www.fortinet.com/blog/threat-research/moveit-transfer-critical-vulnerability-cve-2023-34362-exploited-as-a-0-day
- https://www.bbc.com/mundo/noticias-65834916
- https://news.sophos.com/es-es/2023/06/07/informacion-sobre-la-vulnerabilidad-cve-2023-34362-de-moveit-transfer-y-moveit-cloud/
- https://www.helpnetsecurity.com/2023/06/13/cve-2023-34362-exploit/
- https://github.com/horizon3ai/CVE-2023-34362 PoC (Prueba de concepto)

Cisco publica avisos de seguridad para varios productos

Cisco ha publicado avisos de seguridad sobre vulnerabilidades que afectan a varios productos de Cisco. Un actor remoto de amenazas cibernéticas podría explotar estas vulnerabilidades para tomar el control de un sistema afectado.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.cisa.gov/news-events/alerts/2023/06/13/cisco-releases-security-advisories-multiple-products

---

Actualizaciones de Microsoft de junio

El martes 13 de Junio de 2023 Microsoft genera las actualizaciones de parches de Junio, con actualizaciones de seguridad para 78 fallos, incluidas 38 vulnerabilidades de ejecución remota de código.
Si bien se corrigieron treinta y ocho errores de RCE, Microsoft solo enumeró **seis fallas como "críticas"**, incluidos los ataques de denegación de servicio, la ejecución remota de código y la elevación de privilegios.

Este es el número de errores en cada categoría de vulnerabilidad:

- 17 vulnerabilidades de elevación de privilegios.
- 3 vulnerabilidades de omisión de funciones de seguridad.
- 32 vulnerabilidades de ejecución remota de código.
- 5 vulnerabilidades de divulgación de información.
- 10 vulnerabilidades de denegación de servicio.
- 10 vulnerabilidades de suplantación de identidad.
- 1 vulnerabilidad en Edge por Chromium.

Esta lista no incluye dieciséis vulnerabilidades de Microsoft Edge corregidas previamente el 2 de junio de 2023, con lo cual, darían un resultado final de 94 vulnerabilidades corregidas durante el mes.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2023-patch-tuesday-fixes-78-flaws-38-rce-bugs/
- https://msrc.microsoft.com/update-guide/releaseNote/2023-Jun
- https://www.helpnetsecurity.com/2023/06/13/june-2023-patch-tuesday/

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y/o aplicaciones actualizadas.
- Realizar actualizaciones directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se puede realizar la actualización inmediatamente, dichos controles pueden incluir controles tecnológicos y soluciones de seguridad avanzadas que le permitan minimizar el riesgo de que alguna vulnerabilidad sea explotada.
- Tener una política y un plan de mitigación de vulnerabilidades periódico.
- Contar con soluciones de gestión de vulnerabilidades que le permita hacer la priorización de estas.
- Adquirir tecnologías que le permitan bloquear accesos mal intencionados o intentos de explotación de vulnerabilidades conocidas y de día cero.
- Contar con servicios de Ethical Hacking para identificar posibles superficies de ciberataque antes de que lo hagan sus adversarios, protegiendo los datos sensibles de un uso indebido o de robo, ayudando a prevenir las amenazas en la seguridad de los datos e identificar las vulnerabilidades que pueden ir más allá del sistema perimetral, con el fin de establecer un análisis holístico de las amenazas que puedan comprometer la seguridad de los datos críticos de la compañía, entre otras.

MALWARE

Los usuarios de Minecraft, advertidos de malware dirigido Modpacks

Los jugadores de Minecraft han sido advertidos de la rápida propagación de una campaña de malware en varias fases dirigida a modpacks y plugins.
En un aviso de alerta máxima publicado a las 18.00 BST del 8 de junio, la empresa de ciberseguridad Bitdefender, proporcionó detalles sobre cómo el malware ladrón de información llamado "Fractureiser" se dirige a los usuarios del juego multiplataforma.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/06/11/los-usuarios-de-minecraft-advertidos-de-malware-dirigido-modpacks/

En dos años, LockBit obtiene 91 millones de dólares de víctimas estadounidenses

La infame variante del ransomware LockBit ha hecho ganar a los extorsionadores cerca de 100 millones de dólares solo a víctimas estadounidenses desde enero de 2020, según revelaron las agencias de seguridad aliadas en un nuevo aviso.

La Agencia de Ciberseguridad y Seguridad de Infraestructuras de EE.UU. (CISA), el Centro Nacional de Ciberseguridad del Reino Unido (NCSC) y sus equivalentes australiano, neozelandés, canadiense, francés y alemán redactaron el documento tras advertir de la continua amenaza que supone el colectivo.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/06/16/lockbit-obtiene-91-millones-de-dolares-de-victimas-estadounidenses-en-dos-anos/
- https://www.bleepingcomputer.com/news/security/cisa-lockbit-ransomware-extorted-91-million-in-1-700-us-attacks/

Ataque masivo de ransomware revela la vulnerabilidad de las empresas

El reciente ataque masivo de ransomware perpetrado por el grupo Clop, el cual ha afectado a múltiples organizaciones, resalta la importancia de la educación digital en la prevención de ciberataques y la protección de datos sensibles.

En los últimos días, el grupo de ransomware Clop ha sido noticia por su explotación de una vulnerabilidad crítica en una herramienta corporativa de transferencia de archivos. Esta banda, vinculada a Rusia, ha estado aprovechando una falla de seguridad en MOVEit Transfer, desde finales de mayo.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/06/15/ataque-masivo-de-ransomware-revela-la-vulnerabilidad-de-las-empresas/
- https://therecord.media/shell-impacted-in-clop-ransomware-attack

Recomendaciones generales sobre Malware:

- Controlar de forma minuciosa las conexiones de acceso remoto a su infraestructura: prohíba las conexiones desde redes públicas, permita el acceso RDP solo mediante un canal VPN y use contraseñas seguras y únicas con la autenticación en dos pasos.
- Mantener actualizado el software crítico de manera oportuna, poniendo énfasis en el sistema operativo, las soluciones de seguridad, los clientes de VPN y las herramientas de acceso remoto.
- Mantener a sus empleados constantemente en capacitaciones de concientización de ciberseguridad y en programas de sensibilización de ciberseguridad. En Gamma Ingenieros contamos con un programa completo de sensibilización en ciberseguridad, para obtener más información contacte a su gerente de cuenta, preguntando por nuestro programa de sensibilización y nuestra plataforma propietaria, Gamma Cyberacademy ©.
- Emplear soluciones de ciberseguridad avanzadas para proteger los dispositivos de trabajo y el perímetro de la red corporativa.
- Mantener actualizadas sus soluciones de ciberseguridad.
- Descargar aplicaciones solo de fuentes de confianza, como la tienda oficial de aplicaciones de Google Play Store.
- Revisar las calificaciones y opiniones de otras personas antes de descargar cualquier aplicación, especialmente si es una aplicación bancaria o financiera.
- No responder a llamadas telefónicas de números desconocidos o sospechosos, especialmente si solicitan información personal o financiera.
- No compartir información personal o financiera a través del teléfono o correo electrónico, a menos que esté seguro de la identidad del destinatario.

BRECHAS DE SEGURIDAD

Ransomware Rhysida publica 360.000 documentos del Ejército de Chile

El Ejército de Chile confirmó que se encuentra respondiendo a un ciberataque que afectó a distintos sistemas de la red interna de la organización. El grupo de ransomware se ve a sí mismo como un «equipo de ciberseguridad» que hace un favor a sus víctimas: atacan los sistemas y destacan las «ramificaciones potenciales» de los problemas de seguridad implicados. El grupo amenaza a las víctimas con la distribución pública de los datos exfiltrados en la Dark Web, lo que lo sitúa en la línea de los grupos modernos de «multiextorsión».

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/rhysida-ransomware-leaks-documents-stolen-from-chilean-army/
- https://www.secplicity.org/2023/05/23/scratching-the-surface-of-rhysida-ransomware/

NOTICIAS DE CIBERSEGURIDAD

Killnet, Anonymous Sudan y REvil amenazan con atacar bancos occidentales

Killnet es un grupo con fuertes vínculos "indirectos" los objetivos estratégicos del gobierno ruso, que utiliza principalmente la denegación de servicio distribuida (DDoS) como vector de ataque preferido. Si bien el impacto del grupo ha sido limitado hasta la fecha, existen sólidos indicadores de que Killnet continuará desarrollándose y escalando sus ataques a través de redes maliciosas.En 48 horas, a partir del día Jueves 15 de Junio, los grupos Pro-

Rusos: Killnet, Revil y Anonymous Sudan se han unido para (supuestamente) realizar un ataque masivo al sistema financiero occidental: el objetivo es paralizar los bancos europeos y estadounidenses y el sistema de transferencias internacional SWIFT.

Prioridad: 1 Crítico.

Ampliar información:

- https://blog.segu-info.com.ar/2023/06/killnet-anonymous-sudan-y-revil.html
- https://twitter.com/vxunderground/status/1669053086495563777
- https://blog.elhacker.net/2023/06/killnet-anonymous-sudan-y-revil-amenazan-ataque-bancos.html

---

'Noticias Caracol' y Caracol Televisión sufren duro golpe; hackers se adueñaron de sus cuentas en YouTube y se hacen pasar por Tesla

Un duro golpe han sufrido las cuentas de Noticias Caracol y Caracol Televisión en la red social YouTube, plataforma en la que sus perfiles han sido alterados y parecen estar bajo el dominio de piratas informáticos que utilizan la imagen del multimillonario Elon Musk y Tesla, una de sus compañías.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.semana.com/tecnologia/articulo/noticias-caracol-y-caracol-television-sufren-duro-golpe-hackers-se-aduenaron-de-sus-cuentas-en-importante-red-social/202349/
- https://noticias.caracoltv.com/tecnologia/canales-de-noticias-caracol-y-caracol-television-en-youtube-fueron-hackeados-rg10