GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4523

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín de ciberseguridad semanal 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, tecnología y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	5	1	
MALWARE	1	2	1
NOTICIAS DE CIBERSEGURIDAD	2		2

VULNERABILIDADES

Nueva Vulnerabilidad en CPU de Intel Afecta Entornos Virtualizados Multiinquilino

Intel ha lanzado correcciones para abordar una vulnerabilidad de alta gravedad, denominada Reptar, que afecta a sus CPUs de escritorio, móviles y de servidor. Identificado como CVE-2023-23583 (puntuación CVSS: 8.8), el problema tiene el potencial de "permitir la escalada de privilegios y/o la divulgación de información y/o la denegación de servicio a través de acceso local". La explotación exitosa de la vulnerabilidad podría permitir eludir los límites de seguridad de la CPU, especialmente en entornos virtualizados multiinquilino, donde un atacante podría provocar un bloqueo en la máquina anfitriona, resultando en una denegación de servicio para otras máquinas virtuales en el mismo host. Intel ha publicado microcódigos actualizados como parte de las actualizaciones de noviembre de 2023.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/11/reptar-new-intel-cpu-vulnerability.html

---

Microsoft Publica Parches para 5 Nuevas Vulnerabilidades de Día Cero

Microsoft ha lanzado correcciones para abordar 63 vulnerabilidades de seguridad en su software para el mes de noviembre de 2023, incluyendo tres vulnerabilidades que han sido explotadas activamente. De las 63 fallas, tres son críticas, 56 son importantes y cuatro son moderadas en gravedad. Dos de ellas se conocían públicamente en el momento de la publicación. Cinco vulnerabilidades de día cero notables incluyen problemas en Windows SmartScreen, Windows DWM Core Library, Windows Cloud Files Mini Filter Driver, ASP.NET Core y Microsoft Office. La explotación exitosa podría llevar a la escalada de privilegios, elusión de funciones de seguridad y denegación de servicio.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/11/alert-microsoft-releases-patch-updates.html

---

Vulnerabilidad Crítica no Parcheada en VMware Cloud Director

VMware ha emitido una advertencia sobre una vulnerabilidad crítica y sin parches (CVE-2023-34060, puntuación CVSS: 9.8) en Cloud Director, que podría permitir que un actor malintencionado eluda las restricciones de autenticación. La vulnerabilidad afecta a instancias actualizadas a la versión 10.5 desde versiones más antiguas. Específicamente, un actor de amenazas con acceso a la red del dispositivo podría eludir las restricciones de inicio de sesión en los puertos 22 (SSH) o 5480 (consola de gestión del dispositivo). Aunque aún no hay un parche disponible, VMware ha proporcionado una solución temporal que implica un script de shell ("WA_CVE-2023-34060.sh") sin requerir tiempo de inactividad. Esta alerta sigue a los parches recientes para otra vulnerabilidad crítica en vCenter Server (CVE-2023-34048, puntuación CVSS: 9.8).

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/11/urgent-vmware-warns-of-unpatched.html

---

Nueva Vulnerabilidad en AMD SEV Expone Máquinas Virtuales Encriptadas

Un nuevo ataque llamado CacheWarp ha sido revelado por académicos, afectando la tecnología de Virtualización Segura y Encriptada (SEV) de AMD. Esta vulnerabilidad (CVE-2023-20592) podría permitir a los atacantes infiltrarse en máquinas virtuales encriptadas, logrando escaladas de privilegios y ejecución remota de código. A pesar de que AMD ha lanzado una actualización para corregir el problema, este descubrimiento subraya la importancia de abordar las vulnerabilidades en las tecnologías de virtualización, incluso aquellas diseñadas para proporcionar aislamiento y seguridad avanzada.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/11/cachewarp-attack-new-vulnerability-in.html

---

Zero-Day en el Software de Correo Electrónico Zimbra Explotado por Cuatro Grupos de Hackers

Un defecto zero-day en el software de correo electrónico Zimbra Collaboration fue explotado por cuatro grupos diferentes en ataques del mundo real para robar datos de correo electrónico, credenciales de usuario y tokens de autenticación. La vulnerabilidad, rastreada como CVE-2023-37580 (puntuación CVSS: 6.1), es una vulnerabilidad de scripting entre sitios (XSS) reflejada que afecta a las versiones anteriores a la 8.8.15 Patch 41. Fue abordada por Zimbra como parte de los parches lanzados el 25 de julio de 2023. La explotación exitosa de la falla podría permitir la ejecución

de scripts maliciosos en el navegador web de las víctimas, al engañarlas para que hagan clic en una URL especialmente diseñada, iniciando efectivamente la solicitud XSS a Zimbra y reflejando el ataque de nuevo al usuario.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/11/zero-day-flaw-in-zimbra-email-software.html

---

Vulnerabilidad Crítica en FortiSIEM Permite la Ejecución de Comandos Maliciosos

Fortinet ha alertado sobre una vulnerabilidad crítica de inyección de comandos en su solución de gestión de información y eventos de seguridad, FortiSIEM. La falla (CVE-2023-36553) podría permitir a atacantes remotos no autenticados ejecutar comandos maliciosos a través de solicitudes API manipuladas. Con un puntaje CVSS de 9.3, esta vulnerabilidad, una variante de CVE-2023-34992, afecta a varias versiones de FortiSIEM. La recomendación es que los usuarios actualicen a las versiones especificadas para mitigar el riesgo asociado a esta vulnerabilidad crítica.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/fortisiem-injection-flaw/

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

Grupo de ransomware 8Base despliega nueva variante de Phobos a través de SmokeLoader

El grupo de ransomware 8Base está utilizando una variante del ransomware Phobos en sus ataques, según informes de Cisco Talos. La actividad de 8Base ha aumentado, y la variante de Phobos se distribuye a través del troyano SmokeLoader. Este cargador generalmente descarga cargas útiles adicionales, pero en el caso de 8Base, tiene el componente de ransomware incrustado en sus cargas útiles cifradas. La variante cifra archivos completos menores de 1.5 MB y parcialmente los archivos más grandes para acelerar el proceso de encriptación. 8Base utiliza la extensión ".8base" para los archivos cifrados.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/11/8base-group-deploying-new-phobos.html

Anuncios Maliciosos de Google Engañan a Usuarios de WinSCP para Instalar Malware

Se están utilizando anuncios manipulados de Google para engañar a usuarios de WinSCP, llevándolos a descargar malware en lugar del software legítimo. Los atacantes aprovechan los Anuncios Dinámicos de Búsqueda de Google para dirigir a las víctimas a un sitio web comprometido, gameeweb[.]com, que luego las redirige a un sitio de phishing controlado por los atacantes. La cadena de ataque busca incitar a los usuarios a descargar malware desde un sitio falso de WinSCP, winccp[.]net.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/11/beware-malicious-google-ads-trick.html

---

Descubren 27 Paquetes PyPI Maliciosos con Miles de Descargas Dirigidos a Expertos en TI

Un actor de amenazas desconocido ha estado publicando paquetes "typosquat" en el repositorio Python Package Index (PyPI) durante casi seis meses con el objetivo de entregar malware capaz de ganar persistencia, robar datos sensibles y acceder a billeteras de criptomonedas con fines financieros. Estos 27 paquetes, que se hacían pasar por bibliotecas Python legítimas, atrajeron miles de descargas, con una mayoría de ellas originadas en Estados Unidos, China, Francia, Hong Kong, Alemania, Rusia, Irlanda, Singapur, Reino Unido y Japón. El ataque se caracterizó por el uso de esteganografía para ocultar un payload malicioso dentro de una imagen aparentemente inofensiva, aumentando así la furtividad del ataque. Entre los paquetes afectados se encuentran pyefflorer, pyminor, pyowler, pystallerer, pystob y pywool.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/11/27-malicious-pypi-packages-with.html

---

Nuevo Wiper BiBi-Windows Apunta a Sistemas Windows en Ataques Pro-Hamas

BiBi-Windows Wiper, una versión del malware eliminador utilizado previamente en sistemas Linux contra Israel, ha sido identificado por investigadores de seguridad. Esta variante para Windows, compilada después de la guerra entre Israel y Hamas, sugiere una expansión del ataque a máquinas de usuarios finales y servidores de aplicaciones. El malware sobrescribe archivos en el directorio C:\Users con datos basura, agregando la extensión ".BiBi" a los nombres de archivo, y elimina las copias de seguridad del sistema. Aunque no se ha confirmado su uso en ataques reales, se vincula al grupo hacktivista pro-Hamas llamado Karma y presenta similitudes tácticas con otro actor llamado Moses Staff, presuntamente de origen iraní, en una campaña más amplia contra empresas israelíes con el objetivo de interrumpir sus operaciones mediante la destrucción de datos.

Prioridad: 3 Importante.

Ampliar información:

- https://www.securityweek.com/dropper-service-bypassing-android-security-restrictions-to-install-malware/

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

Vulnerabilidades en Google Workspace y Cloud Platform podrían ser aprovechadas por hackers para ataques de ransomware

Investigadores de seguridad han revelado nuevas formas de ataque contra Google Workspace y Google Cloud Platform que podrían ser explotadas por ciberdelincuentes para realizar ataques de ransomware, exfiltración de datos y recuperación de contraseñas. Estos métodos podrían permitir a los atacantes extender un compromiso de un único dispositivo a toda una red corporativa.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/11/hackers-could-exploit-google-workspace.html

---

Hackers Rusos Vinculados al 'Mayor Ataque Cibernético' contra Infraestructura Crítica Danesa

Hackers rusos, posiblemente vinculados a la agencia militar de inteligencia GRU, llevaron a cabo el "mayor ataque cibernético contra la infraestructura crítica danesa" en mayo de 2023. La coordinada ofensiva se dirigió a 22 empresas del sector energético, explotando una vulnerabilidad crítica en los

firewalls de Zyxel. La agencia de ciberseguridad de Dinamarca, SektorCERT, reveló que los atacantes ejecutaron ataques simultáneos y exitosos, demostrando una planificación avanzada y recursos significativos. La operación sin precedentes llevó a que las organizaciones se desconectaran de internet y adoptaran un modo de aislamiento para protegerse. Los atacantes utilizaron una vulnerabilidad zero-day, y hay evidencia que sugiere la participación de dos grupos de amenazas distintos.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/11/russian-hackers-launch-largest-ever.html

---

La banda de ransomware Medusa afirma haber hackeado Toyota Financial Services

Toyota Financial Services ha confirmado la detección de actividad no autorizada en sistemas, después de que la banda de ransomware Medusa afirmara haber hackeado la compañía. La entidad ha tomado medidas, como poner sistemas afectados fuera de línea y colaborar con las autoridades. La brecha de seguridad parece haberse limitado a Toyota Financial Services Europe & Africa, sin que la compañía haya revelado una violación de datos hasta el momento. La banda Medusa exige un rescate de $8,000,000 y amenaza con filtrar datos robados si no se paga antes del 26 de noviembre. El ataque probablemente aprovechó una vulnerabilidad en Citrix Gateway, con la oficina en Alemania señalada como vulnerable.

Prioridad: 3 Importante.

Ampliar información:

- https://securityaffairs.com/154319/data-breach/toyota-financial-services-medusa-ransomware.html

---

Siete Consejos para Evitar Estafas y Comprar con Seguridad en el Black Friday

Con la llegada del Black Friday, aumenta la locura de compras navideñas, pero también el riesgo de estafas online. Con el comercio electrónico en auge, es crucial protegerse contra estafas, como tiendas falsas que imitan a las legítimas. Verificar la presencia del candado verde en la barra de direcciones, indicando un sitio seguro, es esencial. Además, evitar proporcionar datos personales innecesarios y desconfiar de descuentos excesivos en redes sociales. No utilizar el "social login" para registrar sus datos y mantener la doble autenticación activada cuando sea posible. Finalmente, precaución con el "timo del paquete fantasma" que llega a través de mensajes de texto. Con estos consejos y un antivirus actualizado, se podrs disfrutar del Black Friday de manera segura.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.pandasecurity.com/es/mediacenter/black-friday-cyber-monday-timos/