GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2524

En alianza con

TD SYNNEX FORTINET

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	0	2	2
MALWARE	0	1	3
NOTICIAS DE CIBERSEGURIDAD	0	0	4

VULNERABILIDADES

Vulnerabilidad en SolarWinds CVE-2024-28996

Vulnerabilidad de inyección SWQL de alta gravedad, rastreada bajo CVE-2024-28996 (CVSS 7.5), por Nils Putnins, un evaluador de seguridad afiliado a la Organización del Tratado del Atlántico Norte (OTAN), según informó la empresa junto con el nuevo lanzamiento. Las otras fallas corregidas en la última actualización de SolarWinds incluyen una vulnerabilidad de cross-site scripting de alta gravedad, rastreada bajo CVE-2024-29004).

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/vulnerabilities-threats/solarwinds-flaw-flagged-by-nato-pen-tester

---

Vulnerabilidad Veeam CVE-2024-29855

Veeam identificó una vulnerabilidad de deserialización con CVSS 9.9, que requería autenticación, se descubrió un bypass de autenticación tras una kla realización de una actualización. Sin embargo, los intentos de explotar la vulnerabilidad de deserialización resultaron fallidos, frustrando los esfuerzos del atacante por aprovechar la situación.

Prioridad: 3 Importante.

Ampliar información:

https://summoning.team/blog/veeam-recovery-orchestrator-auth-bypass-cve-2024-29855/

Vulnerabilidad de inyección SQL y ejecución remota de código en Ivanti EPM CVE-2024-29824

Ivanti público un aviso sobre una grave vulnerabilidad de inyección SQL en EPM (endpoint manager) CVE-2024-29824, que permite la ejecución remota de código y tiene una puntuación CVSS de 9.8. La vulnerabilidad permite a los atacantes ejecutar comandos maliciosos en los sistemas afectados. En su comunicado, ZDI e Ivanti detallaron los aspectos técnicos de la vulnerabilidad y proporcionaron una prueba de concepto (POC) para ilustrar su explotación.

Prioridad: 2 Urgente.

Ampliar información:

https://www.horizon3.ai/attack-research/attack-blogs/cve-2024-29824-deep-dive-ivanti-epm-sql-injection-remote-code-execution-vulnerability/

Vulnerabilidad Zero-Day en DNSSEC CVE-2023-50387

Microsoft lanzó un parche esta semana para corregir varias vulnerabilidades, incluida una grave vulnerabilidad de denegación de servicio (DoS) CVE-2023-50387 en el protocolo de Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC), que fue revelada públicamente en febrero.

Prioridad: 2 Urgente.

Ampliar información:

https://www.darkreading.com/vulnerabilities-threats/microsoft-late-dangerous-dnssec-zero-day-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

Troyano "Stealer" instalado a través de KMSPico

En mayo de 2024, la Unidad de Respuesta a Amenazas (TRU) de eSentire detectó un ataque utilizando una herramienta activadora falsa llamada KMSPico, que instala el troyano Vidar Stealer. Alli, el ataque explota dependencias de Java y un script malicioso de AutoIt para desactivar Windows Defender y descifrar la carga útil de Vida mediante una shell. El sitio web kmspico[.]ws, que alojó la herramienta falsa, estuvo detrás de Cloudflare Turnstile y requirió un código para descargar un archivo ZIP, conteniendo el ejecutable malicioso Setuper_KMS-ACTIV.exe. Este ejecutable deshabilitó la supervisión de Windows Defender y descargaó un script de AutoIt que inyectó Vidar Stealer. Vidar utilizaba Telegram como Dead Drop Resolver para almacenar la dirección IP del servidor de comando y control (C2).

Prioridad: 2 Urgente.

Ampliar información:

https://blog.segu-info.com.ar/2024/06/troyano-stealer-instalados-traves-de.html

Nueva campaña de phishing despliega la puerta trasera WARMCOOKIE

Investigadores de ciberseguridad han revelado detalles de una campaña de phishing en curso que utiliza señuelos relacionados con reclutamiento y empleo para distribuir una puerta trasera basada en Windows llamada WARMCOOKIE.

WARMCOOKIE parece ser una herramienta inicial de puerta trasera utilizada para explorar redes de víctimas y desplegar cargas útiles adicionales, dijo el investigador de Elastic Security Labs, Daniel Stepanic.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/06/new-phishing-campaign-deploys.html

---

El ransomware "Black Basta" podría haber explotado una falla Zero-Day en MS Windows

El ransomware "Black Basta" podría haber aprovechado una reciente vulnerabilidad de escalada de privilegios en el Servicio de Informes de Errores de Microsoft Windows, conocida como CVE-2024-26169 (puntuación CVSS: 7.8), según un informe de Symantec. Esta vulnerabilidad, parcheada por Microsoft en marzo de 2024, permitía a los atacantes obtener privilegios de sistema. Symantec descubrió evidencia de que la herramienta de explotación utilizada en los ataques podría haber sido compilada antes del parcheo oficial, indicando la posible explotación de la vulnerabilidad como un zero-day. El grupo responsable, conocido como Cardinal por Symantec y también identificado como Storm-1811 y UNC4393 por la comunidad de ciberseguridad, además, está asociado con motivaciones financieras según el análisis de la empresa.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/06/black-basta-ransomware-may-have.html

---

Malware multiplataforma "Noodle RAT"

Un malware no documentado, conocido como "Noodle RAT" y utilizado por actores de amenazas de habla china durante años, ha sido identificado recientemente en operaciones de espionaje o ciberdelincuencia. Aunque esta puerta trasera fue anteriormente clasificada como una variante de Gh0st RAT y Rekoobe, el investigador de seguridad de Trend Micro, Hara Hiroaki, afirmó que "esta puerta trasera no es simplemente una variante de malware existente, sino un nuevo tipo por completo".

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/06/new-cross-platform-malware-noodle-rat.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

Roban el código fuente del New York Times por un token de GitHub expuesto

El código fuente interno y datos de The New York Times fueron filtrados en el foro de 4chan tras ser robados de los repositorios de GitHub pertenecientes a la compañía en enero de 2024, confirmó The New York Times a BleepingComputer. Los datos, vistos inicialmente por VX-Underground, fueron publicados en un Torrent de 273 GB por un usuario anónimo. Un archivo 'léame' indicó que el robo se realizó usando un token de GitHub expuesto. La filtración incluye 270 GB de código fuente, 5.000 repositorios y 3,6 millones de archivos. Se robó una variedad de información, incluida documentación de TI y el código fuente del juego Wordle.

Prioridad: 3 Importante.
Ampliar información:

https://blog.segu-info.com.ar/2024/06/roban-el-codigo-fuente-del-new-york.html

Actualizaciones de seguridad en junio para todas las empresas

Microsoft lanzó actualizaciones de seguridad para 51 fallas, incluyendo dieciocho vulnerabilidades de ejecución remota de código y una vulnerabilidad Zero-Day divulgada públicamente. Las actualizaciones cubren:

- 25 vulnerabilidades de elevación de privilegios.
- 18 vulnerabilidades de ejecución remota de código.
- 3 vulnerabilidades de divulgación de información.
- 5 vulnerabilidades de denegación de servicio.

El total de 51 fallas no incluye 7 fallas de Microsoft Edge corregidas el 3 de junio. La vulnerabilidad Zero-Day, conocida como "Keytrap," afecta el protocolo DNS y ha sido solucionada con las actualizaciones de hoy. Esta vulnerabilidad, CVE-2023-50868, puede ser explotada para causar una denegación de servicio a través de la validación de DNSSEC.

Prioridad: 3 Importante.

Ampliar información:

https://blog.segu-info.com.ar/2024/06/actualizaciones-de-seguridad-de-junio.html

---

Hackers apoyados por China explotan una vulnerabilidad en Fortinet

Actores de amenazas respaldados por el estado chino accedieron a 20.000 sistemas FortiGate de Fortinet en todo el mundo al explotar una falla de seguridad crítica conocida entre 2022 y 2023, lo que indica un impacto más amplio de lo que se sabía anteriormente.

El actor estatal detrás de esta campaña ya conocía esta vulnerabilidad en los sistemas FortiGate al menos dos meses antes de que Fortinet revelara la vulnerabilidad, confirmó el Centro Nacional de Ciberseguridad de los Países Bajos (NCSC) en un nuevo boletín.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/06/china-backed-hackers-exploit-fortinet.html

---

Hackers norcoreanos apuntan a Fintech brasileña con tácticas sofisticadas de phishing

Actores respaldados por el gobierno norcoreano han apuntado al gobierno brasileño y a los sectores aeroespacial, tecnológico y de servicios financieros de Brasil, dijeron las divisiones Mandiant y TAG de Google en un informe conjunto publicado esta semana. Al igual que en otras regiones, las empresas de criptomonedas, así como las de tecnología financiera han sido un foco particular, al menos tres grupos norcoreanos han dirigido sus ataques a estas empresas brasileñas.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/06/north-korean-hackers-target-brazilian.html