GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °2924

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
VULNERABILIDADES	2	0	0
MALWARE	0	0	3
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Microsoft pide actualizar Windows 10 y 11 cuanto antes: una vulnerabilidad afecta a millones de usuarios de Outlook

Morphisec ha descubierto una vulnerabilidad zero-click, identificada como CVE-2024-38021, que permite la ejecución remota de código en la mayoría de las aplicaciones basadas en Microsoft Outlook. Aunque no se ha detectado explotación reciente, Microsoft advierte que podría haber sido utilizada anteriormente.

Debido a su gravedad, Morphisec ha instado a Microsoft a clasificarla como crítica. La vulnerabilidad afecta a cientos de millones de usuarios de Outlook y puede ser explotada sin ninguna interacción del usuario, lo que complica su detección.

Microsoft ya ha parcheado la vulnerabilidad en las actualizaciones de julio de 2024. Se recomienda a los usuarios actualizar sus sistemas de inmediato para protegerse. La explotación de esta falla podría permitir a los atacantes ejecutar código arbitrario y causar daños significativos.

Prioridad: 1 Crítico.

Ampliar información:

https://www.genbeta.com/actualidad/microsoft-pide-actualizar-windows-10-11-cuanto-antes-vulnerabilidad-afecta-a-millones-usuarios-outlook

---

Vulnerabilidad en los productos Kaspersky CVE-2024-6387, conocida como "regreSSHion"

Kaspersky identificó que algunos productos son vulnerables al CVE-2024-6387 a través de una brecha de seguridad de OpenSSH conocida como "regreSSHion". Esta herramienta, popular para conexiones SSH, tiene más de 14 millones de instancias expuestas, según un análisis de Shodan y Censys, que podrían ser vulnerables a dicha falla.

La vulnerabilidad CVE-2024-6387 permite la ejecución de código mediante la explotación de una condición de carrera en instalaciones por defecto de OpenSSH. Aunque el impacto es crítico (RCE como usuario root), el riesgo se considera "alto" debido a la complejidad de su ejecución, que requiere múltiples intentos durante un largo periodo.

La explotación en sistemas Linux se relaciona con el uso de syslog y funciones inseguras como malloc y free. Sin embargo, los sistemas OpenBSD no se ven afectados gracias a su versión segura de syslog. Se recomienda a los administradores de sistemas que mantengan sus instalaciones de OpenSSH actualizadas para mitigar esta vulnerabilidad.

Prioridad: 1 Crítico.

Ampliar información:

https://www.tarlogic.com/es/blog/cve-2024-6387-vulnerabilidad-regresshion-afecta-openssh

https://support.kaspersky.com/vulnerability/list-of-advisories/12430#120724/

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

ClickFix Deception: una táctica de ingeniería social para implementar malware

McAfee Labs ha identificado un método inusual de distribución de malware denominado "Clickfix". Este ataque comienza atrayendo a los usuarios a sitios web aparentemente legítimos pero infectados, que luego redirigen a las víctimas a dominios con ventanas emergentes falsas. Estas ventanas emergentes instan a los usuarios a pegar un script en una terminal de PowerShell.

"Clickfix" es una técnica de ingeniería social sofisticada que se aprovecha de la apariencia de autenticidad para engañar a los usuarios y hacer que ejecuten scripts maliciosos. Los sitios web comprometidos están diseñados para parecer genuinos, aumentando la probabilidad de que los usuarios sigan las instrucciones. Una vez que el script se ejecuta en PowerShell, el malware se infiltra en el sistema de la víctima, lo que puede resultar en robo de datos, compromisos del sistema o una mayor propagación del malware.

Prioridad: 3 Importante.

Ampliar información:

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clickfix-deception-a-social-engineering-tactic-to-deploy-malware/

La versión 4.0 del ransomware HardBit admite nuevas técnicas de ofuscación

La versión 4.0 del ransomware HardBit introduce mejoras significativas en la ofuscación binaria y protección mediante contraseña. Este ransomware requiere una contraseña al ejecutarse y ofrece versiones tanto CLI como GUI, facilitando su uso por operadores con menos habilidades técnicas.

HardBit se distribuye a través del virus Neshta y es un binario .NET, oculto con el empaquetador personalizado Ryan-_-Borland_Protector Cracked v1.0. A diferencia de otros ransomware, HardBit no usa el modelo de doble extorsión y amenaza con nuevos ataques si no se paga el rescate. Las víctimas deben contactar al grupo por correo electrónico o Tox.

Prioridad: 3 Importante

Ampliar información:

https://securityaffairs.com/165735/malware/hardbit-ransomware-version-4-0.html

---

La campaña de malware "DarkGate" utiliza recursos compartidos de archivos samba

La Unidad 42 de Palo Alto Networks ha revelado detalles sobre una campaña de malware denominada "DarkGate", que tuvo lugar de marzo a abril de 2024. Los atacantes usaron archivos de Microsoft Excel para descargar software malicioso desde recursos compartidos de archivos SMB públicos.

DarkGate RAT, escrito en Borland Delphi y disponible como Malware as a Service (MaaS), es una amenaza sofisticada y en constante mejora. Activo desde 2018, DarkGate admite funciones como inyección de procesos, robo de información y registro de teclas, empleando técnicas avanzadas de evasión.

Prioridad: 3 Importante.

Ampliar información:

https://securityaffairs.com/165723/malware/dark-gate-malware-uses-samba-file-shares.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

Los piratas informáticos de CRYSTALRAY infectan a más de 1.500 víctimas mediante una herramienta de mapeo de red

Un actor de amenazas, identificado como CRYSTALRAY por Sysdig, ha ampliado sus operaciones, infectando a más de 1.500 víctimas. Sus actividades, que han aumentado diez veces, incluyen escaneo masivo, explotación de vulnerabilidades y colocación de puertas traseras usando herramientas de seguridad de código abierto. Los ataques están dirigidos

a recolectar y vender credenciales, implementar mineros de criptomonedas y mantener el acceso persistente en los sistemas afectados.

Prioridad: 3 Importante.

Ampliar información:

https://www.redpacketsecurity.com/crystalray-hackers-infect-over-1-500-victims-using-network-mapping-tool/

El nuevo kit antiphishing FishXProxy permite que los Script Kiddies accedan al phishing

Un ataque de cadena de suministro dirigido a la biblioteca JavaScript ampliamente utilizada Polyfill[.]io ha afectado a más de 380,000 hosts según nuevos hallazgos de Censys. El ataque involucra la inserción de un script polyfill vinculado a dominios maliciosos como "https://cdn.polyfill[.]io" o "https://cdn.polyfill[.]com" en las respuestas HTTP de estos hosts. En particular, aproximadamente 237,700 de estos hosts están ubicados en la red de Hetzner en Alemania (AS24940), una popular plataforma de alojamiento web. Este incidente destaca la vulnerabilidad de las cadenas de suministro digitales y la necesidad de medidas robustas de seguridad cibernética para proteger contra estos ataques.

Prioridad: 3 Importante.

Ampliar información:

https://hackread.com/new-fishxproxy-phishing-kit-script-kiddies/?web_view=true

---