GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

En alianza con

TD SYNNEX FORTINET

Edición °3824

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

VULNERABILIDADES

Vulnerabilidad crítica en SonicWall SSLVPN explotada en ataques de Ransomware CVE-2024-40766

Una vulnerabilidad crítica en los dispositivos de firewall SonicWall, identificada como CVE-2024-40766, está siendo explotada por actores de ransomware, particularmente el grupo Akira. Esta vulnerabilidad, con una puntuación CVSS de 9.3, afecta a los dispositivos SonicWall Gen 5, Gen 6 y Gen 7 que utilizan SonicOS. La falla permite a los atacantes evadir controles de acceso, logrando comprometer cuentas locales en las que se ha deshabilitado la autenticación multifactor (MFA). A través de estos accesos no autorizados, los atacantes pueden implantar ransomware en las redes objetivo.

SonicWall lanzó parches el 22 de agosto de 2024, advirtiendo inicialmente que el problema se limitaba al acceso de gestión, pero luego reveló que también afecta la funcionalidad SSLVPN, lo que amplifica su gravedad. Se recomienda a los administradores aplicar los

parches lo antes posible, restringir el acceso al portal de administración a fuentes confiables y habilitar MFA para todas las cuentas SSL VPN.

Prioridad: 1 Crítico.

Ampliar información:

https://www.bleepingcomputer.com/news/security/critical-sonicwall-sslvpn-bug-exploited-in-ransomware-attacks/

GitLab alerta sobre una vulnerabilidad crítica en la ejecución de pipelines CVE-2024-6678

GitLab ha emitido una advertencia sobre una vulnerabilidad crítica (CVE-2024-6678) que afecta a las versiones 8.14 a 17.3.2 de GitLab Community y Enterprise Edition (CE/EE). Esta falla, con un puntaje CVSS de 9.9, permite a atacantes ejecutar pipelines como otros usuarios, lo que podría comprometer entornos con permisos elevados sin requerir interacción del usuario.

Para mitigar el riesgo, GitLab ha lanzado parches en las versiones 17.3.2, 17.2.5 y 17.1.7, y recomienda a los usuarios actualizar inmediatamente para evitar posibles explotaciones.

Prioridad: 1 Crítico.

Ampliar información:

https://www.bleepingcomputer.com/news/security/gitlab-warns-of-critical-pipeline-execution-vulnerability/

Adobe corrige vulnerabilidad de día cero en Acrobat Reader con exploit público

Adobe ha solucionado una vulnerabilidad crítica de día cero en Acrobat Reader, conocida como CVE-2024-41869, que ya estaba siendo explotada activamente con un exploit de prueba de concepto (PoC) público. Esta vulnerabilidad es del tipo *use after free*, lo que significa que los atacantes pueden ejecutar código remoto al abrir archivos PDF maliciosos. El problema surge cuando el programa intenta acceder a una ubicación de memoria que ya ha sido liberada, lo que puede llevar a la ejecución de código malicioso. La vulnerabilidad afecta tanto a usuarios de Windows como macOS, y Adobe ya ha lanzado actualizaciones que corrigen el fallo.

La recomendación principal es que los usuarios y administradores actualicen Adobe Acrobat Reader y Acrobat a la última versión lo antes posible para mitigar los riesgos. Esta actualización es especialmente urgente dado que el exploit ha sido demostrado públicamente, lo que aumenta el riesgo de ataques masivos. Es aconsejable habilitar las actualizaciones automáticas para recibir futuros parches sin intervención manual.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/adobe-fixes-acrobat-reader-zero-day-with-public-poc-exploit/

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

Malware bloquea el navegador en modo kiosco para robar credenciales de Google

Investigadores de Lumens Black Lotus Labs identificaron un malware llamado *StealC* que bloquea navegadores en modo kiosco para capturar credenciales de Google. Este malware fuerza a las víctimas a ingresar sus credenciales al bloquear el navegador en la página de inicio de sesión de Google, sin posibilidad de cerrarlo fácilmente. Se propaga principalmente mediante sitios web comprometidos o descargas de software malicioso. Para mitigar el riesgo, se recomienda cerrar el navegador con "Alt+F4" y evitar el uso de credenciales en entornos sospechosos.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/malware-locks-browser-in-kiosk-mode-to-steal-google-credentials/

Hadooken: nuevo malware para Linux ataca servidores Oracle WebLogic

Investigadores de Aqua Security han descubierto una nueva amenaza llamada "Hadooken", un malware dirigido a servidores Oracle WebLogic que aprovecha credenciales débiles para acceder a estos entornos críticos. Este malware se propaga principalmente mediante scripts descargados tras obtener acceso inicial al servidor, y posteriormente despliega un cryptominer y el botnet Tsunami para ataques de denegación de servicio distribuido (DDoS). Se ha vinculado a actividades de minería de criptomonedas y ataques de red en sistemas Linux, aunque también se ha identificado la posibilidad de ataques de ransomware en sistemas Windows. El malware se esconde en procesos disfrazados de aplicaciones legítimas, dificultando su detección y análisis forense.

Para mitigar este tipo de ataques, los expertos recomiendan fortalecer las credenciales de acceso, aplicar parches de seguridad en los servidores Oracle WebLogic y monitorear actividades sospechosas en los logs del sistema. Es crucial eliminar las configuraciones predeterminadas y asegurar el acceso a través de autenticación multifactor (MFA) y el uso de firewalls efectivos. Dado que Hadooken también puede borrar los registros del sistema para evitar la detección, implementar soluciones de monitoreo continuo es esencial para prevenir futuras intrusiones

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/new-linux-malware-hadooken-targets-oracle-weblogic-servers/

Ajina.Banker: malware que roba datos financieros y evade 2FA mediante Telegram

El malware Ajina.Banker, identificado por Group-IB, se dirige a usuarios de bancos en Asia Central. Este software malicioso se propaga a través de canales de Telegram, haciéndose pasar por aplicaciones legítimas de servicios bancarios o gubernamentales. Una vez instalado, roba información financiera y 2FA, exfiltrando datos a servidores remotos. Utiliza permisos del sistema como SMS y aplicaciones financieras para maximizar su impacto. Para mitigar, se recomienda evitar instalar aplicaciones de fuentes no confiables y usar Google Play Protect.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/09/new-android-malware-ajinabanker-steals.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

WordPress exigirá 2FA para desarrolladores de plugins a partir de octubre

A partir del 1 de octubre, WordPress.org requerirá que los desarrolladores de plugins y temas activen la autenticación de dos factores (2FA) en sus cuentas. Esta medida, identificada por el equipo de revisión de plugins, busca reducir el riesgo de ataques a la cadena de suministro al prevenir accesos no autorizados a cuentas con permisos para publicar actualizaciones. El malware o el código malicioso podría integrarse en millones de sitios web si las cuentas no son seguras.
Para mitigar estos riesgos, además de activar 2FA, WordPress implementará contraseñas específicas para Subversion (SVN), separando los permisos de acceso a cambios de código de las credenciales de la cuenta principal. Se recomienda a los desarrolladores que actualicen scripts de implementación como GitHub Actions al usar estas nuevas credenciales.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/wordpressorg-to-require-2fa-for-plugin-developers-by-october/

Vulnerabilidad en Apple Vision Pro expone entradas del teclado virtual a atacantes

Investigadores de la Universidad de Florida y el equipo CertiK identificaron la vulnerabilidad GAZEploit en el dispositivo Apple Vision Pro. Este ataque permite a un actor malicioso inferir entradas del teclado virtual mediante el análisis de los movimientos oculares del usuario. El fallo, catalogado como CVE-2024-40865, afectaba la funcionalidad "Persona" del sistema visionOS.
Apple lanzó una actualización en julio de 2024 para corregir este problema, desactivando el avatar virtual cuando el teclado está activo. Se recomienda mantener actualizado el software y evitar compartir sesiones de avatar virtual.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/09/apple-vision-pro-vulnerability-exposed.html

---