GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

En alianza con

TD SYNNEX FORTINET

Edición °3024

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

VULNERABILIDADES

Vulnerabilidades múltiples en productos de Oracle

Se han identificado múltiples vulnerabilidades en varios productos de Oracle, incluyendo Oracle MySQL, Java SE, Oracle Database Server, WebLogic Server y VirtualBox. Estas vulnerabilidades permiten a un atacante remoto causar condiciones de denegación de servicio, divulgación de información sensible, manipulación de datos y eludir restricciones de seguridad en los sistemas afectados. Se recomienda aplicar las correcciones emitidas por el proveedor y consultar los detalles en el sitio web de Oracle.

Prioridad: 2 Urgente.

Ampliar información:

https://www.hkcert.org/security-bulletin/oracle-products-multiple-vulnerabilities_20240717

Vulnerabilidades múltiples en productos de Cisco

Se han identificado múltiples vulnerabilidades en productos de Cisco, incluyendo Cisco AsyncOS para Secure Email Gateway versiones 15.0, 14.2 y anteriores. Estas vulnerabilidades permiten a un atacante remoto causar condiciones de denegación de servicio, ejecución remota de código, elevación de privilegios y manipulación de datos en los sistemas afectados. Se recomienda aplicar las correcciones emitidas por el proveedor, consultando los detalles en el sitio web de Cisco.

Prioridad: 2 Urgente.

Ampliar información:

https://www.hkcert.org/security-bulletin/cisco-products-multiple-vulnerabilities_20240718

Vulnerabilidad Zero-Day en Telegram permite envío de APKs maliciosas como videos

Una vulnerabilidad zero-day en Telegram para Android, denominada 'EvilVideo', permitió a los atacantes enviar cargas útiles maliciosas de APK disfrazadas de archivos de video. Descubierta por investigadores de ESET tras una demostración de prueba de concepto, la

falla existía en Telegram v10.14.4 y versiones anteriores. El exploit fue vendido por el actor de amenazas 'Ancryno' en un foro de hacking de habla rusa el 6 de junio de 2024. ESET notificó a Telegram, que solucionó el problema en la versión 10.14.5, lanzada el 11 de julio de 2024. Aunque no está claro si la vulnerabilidad fue explotada activamente, se encontraron APKs maliciosos en VirusTotal que se hacían pasar por Avast Antivirus y xHamster Premium Mod. La vulnerabilidad permitía que los archivos APK maliciosos aparecieran como videos embebidos en Telegram, engañando a los usuarios para que los descargaran y ejecutaran.

Prioridad: 1 Crítico.

Ampliar información:

https://www.bleepingcomputer.com/news/security/telegram-zero-day-allowed-sending-malicious-android-apks-as-videos/#google_vignette

---

SolarWinds corrige vulnerabilidades críticas en Access Rights Manager

SolarWinds ha lanzado parches para 13 vulnerabilidades en Access Rights Manager, incluyendo ocho de severidad crítica. Seis de estas fallas críticas pueden ser explotadas para la ejecución remota de código, mientras que las otras dos permiten la lectura y eliminación de archivos arbitrarios. Reportadas en enero a través de la Iniciativa Zero Day de Trend Micro, estas vulnerabilidades afectan la versión 2023.2.4 y anteriores. Fueron corregidas en la versión 2024.3. Se recomienda a los usuarios actualizar el software lo antes posible.

Prioridad: 1 Crítico.

Ampliar información:

https://www.securityweek.com/solarwinds-patches-critical-vulnerabilities-in-access-rights-manager/

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

Nuevo malware “Poco RAT” utiliza archivos 7zip en Google Drive

El malware Poco RAT, descubierto a principios de 2024, se disfraza dentro de archivos 7zip hospedados en Google Drive para evadir medidas de seguridad y entregar su carga maliciosa. Dirigido principalmente a hablantes de español en la industria minera, Poco RAT utiliza enlaces directos y embebidos en correos electrónicos y archivos PDF para distribuirse. A pesar de sus intentos de evadir la detección, el malware presenta tasas de detección promedio del 38% para ejecutables y 29% para archivos comprimidos. Poco RAT establece persistencia mediante claves del registro, se inyecta en procesos legítimos y se comunica con un servidor C2 para ejecutar y descargar malware adicional.

Prioridad: 2 Urgente.

Ampliar información:

https://gbhackers.com/poco-rat-7zip-google-drive/#google_vignette

---

Incidente de CrowdStrike aprovechado para phishing, estafas y entrega de malware

El reciente incidente de CrowdStrike, que causó una caída masiva en sistemas Windows debido a una actualización defectuosa, ha sido explotado por actores maliciosos para phishing, estafas y distribución de malware. Los delincuentes han utilizado archivos maliciosos disfrazados como 'hotfixes' para entregar cargas útiles como HijackLoader y Remcos, un RAT que permite el control remoto de dispositivos infectados. Además, se han registrado numerosos dominios relacionados con CrowdStrike para alojar páginas de phishing y ofrecer soluciones falsas que requieren pagos en criptomonedas. Agencias gubernamentales han emitido alertas para que usuarios y organizaciones se mantengan vigilantes y eviten seguir instrucciones de fuentes no verificadas.

Prioridad: 1 Crítico.

.

Ampliar información:

https://www.securityweek.com/crowdstrike-incident-leveraged-for-malware-delivery-phishing-scams/

Malware SocGholish utilizado para difundir AsyncRAT y BOINC

El malware SocGholish (también conocido como FakeUpdates) está siendo utilizado para distribuir AsyncRAT y una instalación maliciosa del proyecto BOINC. SocGholish descarga un AsyncRAT variante sin archivos y una versión modificada de BOINC desde un servidor malicioso. Mientras que BOINC es una plataforma de computación distribuida legítima, en este caso se configura para conectarse a servidores falsos, permitiendo la recopilación de datos y la ejecución de tareas remotas. Los investigadores han observado que, a pesar de que muchos clientes se conectan a estos servidores falsos, no se han ejecutado tareas, lo que sugiere que el proyecto BOINC está siendo utilizado como una fachada para operaciones de comando y control (C2).

Prioridad: 3 Importante.

Ampliar información:

https://securityaffairs.com/166030/malware/socgholish-used-deliver-asyncrat.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

Microsoft lanza herramienta para recuperar equipos dañados por CrowdStrike

Microsoft ha lanzado una herramienta de recuperación personalizada de WinPE para encontrar y eliminar una actualización defectuosa de CrowdStrike que bloqueó alrededor de 8,5 millones de dispositivos Windows. Los administradores debían reiniciar los dispositivos afectados en Modo seguro o Entorno de recuperación para eliminar manualmente el controlador del kernel defectuoso. Dada la magnitud del problema, Microsoft creó una herramienta que automatiza este proceso, facilitando la recuperación de los dispositivos. La herramienta está disponible en el Centro de descarga de Microsoft y requiere un cliente Windows de 64 bits, una unidad USB de al menos 1 GB y, si es necesario, una clave de recuperación Bitlocker. La herramienta formatea la unidad USB, crea una imagen WinPE personalizada y, al iniciar el dispositivo afectado con esta unidad, elimina automáticamente el controlador defectuoso.

Prioridad: 1 Crítico.

Ampliar información:

https://blog.segu-info.com.ar/2024/07/herramienta-de-microsoft-para-recuperar.html

---

Grupos de hackers abusan de Google Cloud para phishing de credenciales

Los grupos de hackers PINEAPPLE y FLUXROOT están utilizando proyectos sin servidor de Google Cloud para llevar a cabo actividades de phishing de credenciales. FLUXROOT ha creado páginas de phishing en Google Cloud para robar información de inicio de sesión de usuarios de Mercado Pago, mientras que PINEAPPLE ha utilizado instancias comprometidas para propagar el malware Astaroth en Brasil. Google ha respondido eliminando los proyectos maliciosos y actualizando sus listas de Navegación Segura para mitigar estas amenazas.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/07/pineapple-and-fluxroot-hacker-groups.html

---