GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

En alianza con

TD SYNNEX FORTINET

Edición °3424

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

VULNERABILIDADES

Zoom corrige vulnerabilidades críticas que permiten escalada de privilegios

Zoom ha revelado varias vulnerabilidades críticas que afectan sus aplicaciones de Workplace, SDKs y clientes de Rooms, poniendo en riesgo a usuarios en múltiples plataformas. Entre las más graves se encuentran CVE-2024-39825 y CVE-2024-39818, con un puntaje CVSS de 8.5, que podrían permitir a atacantes escalar privilegios. Estos fallos impactan a versiones anteriores a la 6.0.0 de Zoom en Windows, macOS, Linux, iOS y Android. Zoom ha lanzado parches para mitigar estos riesgos y recomienda a los usuarios actualizar sus aplicaciones de inmediato.

Prioridad: 2 Urgente.

Ampliar información:

https://gbhackers.com/zoom-fixes-vulnerabilities/

Vulnerabilidad en Outlook permite ejecución remota de código con solo hacer clic en un correo

Investigadores de NetSPI han descubierto una vulnerabilidad crítica en Microsoft Outlook (CVE-2024-21378) que permite la ejecución remota de código con solo hacer clic en un correo electrónico. El fallo se debe a una validación incorrecta de objetos de formularios sincronizados, lo que permite a los atacantes registrar y ejecutar un ejecutable malicioso mediante rutas relativas en el registro. Aunque Microsoft ha lanzado un parche para mitigar este problema, la documentación oficial aún no ha sido actualizada. Además, se identificó otra vulnerabilidad (CVE-2024-30103) que también ha sido corregida.

Prioridad: 1 Crítico.

Ampliar información:

https://gbhackers.com/0-click-outlook-rce-vulnerability/

Vulnerabilidades críticas en IBM QRadar permiten la ejecución remota de código arbitrario

IBM ha revelado vulnerabilidades críticas en su software QRadar Suite y Cloud Pak for Security que podrían permitir a los atacantes ejecutar código arbitrario de forma remota, comprometiendo gravemente la seguridad. Las vulnerabilidades incluyen un fallo de deserialización en Node.js que podría causar una denegación de servicio y una vulnerabilidad de contaminación de prototipos en fast-loops, con una puntuación CVSS de 9.8. IBM insta a los usuarios a actualizar a la versión 1.10.24.0 o superior para mitigar estos riesgos y proteger sus sistemas.

Prioridad: 1 Crítico.

Ampliar información:

https://gbhackers.com/ibm-qradar-allow-attackers/

Adobe llama la atención sobre un conjunto masivo de fallos de ejecución de código

Adobe ha lanzado correcciones para 72 vulnerabilidades de seguridad en múltiples productos, advirtiendo que los usuarios de Windows y macOS están en riesgo de sufrir ejecuciones de código, fugas de memoria y ataques de denegación de servicio. Entre los productos afectados se encuentran Adobe Acrobat, Reader, Illustrator, Photoshop, InDesign, y otros. Las vulnerabilidades más graves podrían permitir a los atacantes tomar control total de una máquina objetivo. Adobe insta a los usuarios a actualizar sus sistemas inmediatamente para mitigar estos riesgos.

Prioridad: 2 Urgente.

Ampliar información:

https://www.securityweek.com/adobe-calls-attention-to-massive-batch-of-code-execution-flaws/

Zero-Day Copy2Pwn explotado para eludir protecciones de Windows

Trend Micro's Zero Day Initiative (ZDI) ha detallado una vulnerabilidad de día cero, denominada Copy2Pwn y rastreada como CVE-2024-38213, que fue explotada por ciberdelincuentes para eludir las protecciones de Windows. La vulnerabilidad, que fue parcheada por Microsoft en junio de 2024 y revelada con las actualizaciones de Patch Tuesday de agosto, permite a los atacantes evadir Defender SmartScreen, así como otras protecciones de seguridad al copiar y pegar archivos desde WebDAV shares sin que se les asigne la marca de origen (MotW). Este fallo crítico fue descubierto en ataques de la campaña DarkGate, dirigida por el grupo Water Hydra.

Prioridad: 2 Urgente.

Ampliar información:

https://www.securityweek.com/copy2pwn-zero-day-exploited-to-bypass-windows-protections/

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

Nueva campaña de malspam ataca AnyDesk y Microsoft Teams

Investigadores de ciberseguridad han detectado una campaña de malspam que utiliza plataformas como AnyDesk y Microsoft Teams para comprometer los sistemas de las víctimas. Los atacantes envían un aluvión de correos electrónicos y luego realizan una llamada telefónica a través de Microsoft Teams, haciéndose pasar por representantes legítimos. Convencen a las víctimas para que instalen AnyDesk, ganando así acceso remoto completo a sus equipos. Una vez comprometidos, ejecutan cargas maliciosas para robar datos sensibles.

Prioridad: 2 Urgente.

Ampliar información:

https://gbhackers.com/malspam-attacks-anydesk-microsoft/

BeaverTail Malware ataca a usuarios de Windows a través de juegos

Investigadores de Group-IB han identificado una nueva campaña de malware llamada BeaverTail, atribuida al grupo Lazarus de Corea del Norte. Inicialmente centrado en macOS, BeaverTail ha evolucionado para atacar a usuarios de Windows mediante juegos manipulados con código malicioso. Este malware, que se oculta en paquetes de NPM y se disfraza como aplicaciones legítimas, tiene como objetivo robar datos confidenciales, incluyendo información de criptomonedas y extensiones de navegador. Los usuarios están en riesgo de perder activos digitales a través de ataques sofisticados que explotan software de comunicación y juegos populares.

Prioridad: 3 Importante.

Ampliar información:

https://gbhackers.com/beavertail-malware-weaponized-games-attack/

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

BlindEagle: La Amenaza Persistente en América Latina

El grupo de ciberespionaje BlindEagle, también conocido como APT-C-36, sigue siendo una amenaza significativa en América Latina, especialmente en Colombia, Ecuador, Chile y Panamá. Utilizan técnicas de phishing para distribuir malware, enfocándose tanto en el robo de credenciales financieras como en espionaje. Su metodología ha evolucionado, incluyendo el uso de RATs de código abierto y técnicas de ofuscación, lo que les permite

adaptar sus ataques. Recientes campañas indican su capacidad de cambiar tácticas con el fin de colaborar con terceros para aumentar su alcance y sofisticación.

Prioridad: 1 Crítico.

Ampliar información:

https://securelist.com/blindeagle-apt/113414/

Nuevo exploit BYOVDLL Bypasa la Protección de LSASS en Windows

Investigadores de Orange Cyberdefense descubrieron un nuevo exploit denominado BYOVDLL (Bring Your Own Vulnerable DLL) que permite a los atacantes evadir la protección de LSASS en Windows. Este método aprovecha vulnerabilidades no parcheadas en las bibliotecas keyiso.dll y ncryptprov.dll, permitiendo la ejecución de código arbitrario sin necesidad de reiniciar el sistema. Aunque Microsoft intentó corregir el fallo con actualizaciones anteriores, el exploit BYOVDLL demuestra la persistencia de las vulnerabilidades en procesos críticos de Windows, como LSASS, subrayando los desafíos en la defensa contra vectores de ataque avanzados.

Prioridad: 2 Urgente.

Ampliar información:

https://gbhackers.com/byovdll-exploit-bypassing-lsass-protection/
