GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

En alianza con

TD SYNNEX FORTINET

Edición °3224

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

VULNERABILIDADES

Aumento de la actividad contra Apache OFBiz CVE-2024-32113

En mayo de este año, se publicó una actualización de seguridad crítica para OFBiz. Esta actualización solucionó una vulnerabilidad de recorrido de ruta que podía llevar a la ejecución remota de comandos. Las versiones de OFBiz anteriores a la 18.12.13 se vieron afectadas. Unas semanas después, se hicieron públicos los detalles sobre la vulnerabilidad.

La vulnerabilidad de Directory traversal se puede activar fácilmente insertando un punto y coma. Un atacante solo necesita encontrar una URL accesible y agregar un punto y coma seguido de una URL restringida.

Prioridad: 3 Importante.

Ampliar información:

https://isc.sans.edu/diary/Increased%20Activity%20Against%20Apache%20OFBiz%20CVE-2024-32113/31132?&web_view=true

---

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

El nuevo malware LianSpy se oculta bloqueando una función de seguridad de Android

Se ha descubierto un malware no documentado para Android, previamente llamado 'LightSpy', el cual apunta a usuarios rusos y se hace pasar por una aplicación de Alipay o un servicio del sistema en los teléfonos para evadir la detección. El análisis muestra que este malware ha estado apuntando activamente a los usuarios de Android desde julio de 2021, pero sus amplias capacidades de sigilo lo ayudaron a permanecer sin ser detectado durante más de tres años. Los investigadores de Kaspersky creen que los actores de amenazas utilizan una vulnerabilidad de día cero o tienen acceso físico para infectar dispositivos con el malware. LightSpy obtiene privilegios de root en el dispositivo para tomar capturas de pantalla, robar archivos y recopilar registros de llamadas.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/new-lianspy-malware-hides-by-blocking-android-security-feature/

Nueva campaña DEV#POPPER entregan malware dirigido a los desarrolladores para afectar sistemas Linux, Windows y macOS

La campaña DEV#POPPER se enfoca en distribuir malware a sistemas operativos Linux, Windows y macOS. Los atacantes apuntan principalmente a desarrolladores de software, utilizando técnicas sofisticadas de ingeniería social y métodos para ejecutar código malicioso.

Prioridad: 3 Importante.

Ampliar información:

https://csirtasobancaria.com/nuevo-rat-para-android-denominado-bingomod-efectuando-transacciones-bancarias/nueva-campana-dev-popper-entregan-malware-dirigido-a-los-desarrolladores-para-afectar-sistemas-linux-windows-y-macos

---

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

El aumento de los ataques del Ransomware Magniber afecta a usuarios domésticos de todo el mundo

Está en marcha una campaña masiva de ransomware Magniber, que cifra los dispositivos de usuarios domésticos en todo el mundo y exige rescates de mil dólares para recibir un descifrador. Magniber se lanzó en 2017 como sucesor de la operación ransomware Cerber, cuando se detectó que era distribuido por el kit de explotación Magnitude. Desde entonces, la operación de ransomware ha experimentado ráfagas de actividad a lo largo de los años, y los actores de la amenaza han utilizado varios métodos para distribuir Magniber, cifrando los dispositivos. Estas tácticas incluyen el uso de ataques de día cero de Windows, actualizaciones falsas de Windows, así como cracks de software troyanizados y generadores de claves.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/surge-in-magniber-ransomware-attacks-impact-home-users-worldwide/?&web_view=true

---

Black Basta desarrolla malware personalizado tras el desmantelamiento de Qakbot

Uno de los nuevos métodos de acceso inicial emplea una puerta trasera llamada SilentNight, que el grupo utilizó en 2019 y 2021 antes de archivarla hasta el año pasado. A principios de este año, el grupo comenzó a reactivar SilentNight en sus campañas de publicidad maliciosa, lo que representa un cambio significativo respecto al phishing, que había sido el único método conocido para el acceso inicial, según los investigadores.

SilentNight es una puerta trasera escrita en C/C++ que se comunica a través de HTTP/HTTPS y emplea un algoritmo de generación de dominios para el comando y control (C2). Posee un marco modular que permite la integración de complementos para ofrecer una variedad de funcionalidades, como control del sistema, captura de pantalla, registro de teclas, administración de archivos y acceso a billeteras de criptomonedas. Además, también ataca las credenciales manipulando el navegador.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/threat-intelligence/black-basta-develops-custom-malware-in-wake-of-qakbot-takedown

---

El APT chino StormBamboo comprometió a un proveedor de servicios de Internet y envió malware

Investigadores de Volexity han revelado que el grupo APT StormBamboo, también conocido como "Evasive Panda", "Daggerfly" y "StormCloud", ha comprometido con éxito un proveedor de servicios de Internet (ISP) no especificado para envenenar las respuestas de DNS dirigidas a organizaciones objetivo. Utilizando mecanismos inseguros de actualización de software, los atacantes instalaron malware en dispositivos macOS y Windows de las víctimas.

Prioridad: 3 Importante.

Ampliar información:

https://securityaffairs.com/166552/apt/stormbamboo-compromised-isp-malware.html