Boletín de Ciberseguridad N°70

Fecha de publicación: 13/11/2023

Mes de noviembre

30/10/2023 – 13/11/2023

Datasec

BOLETÍN DE CIBERSEGURIDAD

Indice

Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención. La publicación de dichas noticias dependerá de la importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta primera quincena del mes de noviembre se destacan 6 noticias de relevancia, siendo estas sobre vulnerabilidades tecnológicas.

Aquellas noticias a tener especial recaudo son las siguientes:

Alerta de Día Cero: Lace Tempest Explota Vulnerabilidad en Software SysAid

Alerta de día cero: Lace Tempest aprovecha la vulnerabilidad del software de soporte de TI SysAid.

Descubren Minero de Criptomonedas Indetectable en Azure Automation

Investigadores descubren una técnica de criptominería indetectable en Azure Automation

Alerta CISA: Explotación Activa de Vulnerabilidad SLP de Alta Gravedad"

CISA: Vulnerabilidad SLP de alta gravedad ahora bajo explotación activa.

Vulnerabilidad Crítica

VEEAM	Vulnerabilidades críticas en Software de Monitoreo Veeam	CRÍTICO

Descripción

Defectos críticos descubiertos en el software de monitoreo de TI Veeam ONE.

Estado

Veeam ha lanzado actualizaciones de seguridad para abordar cuatro fallas en su plataforma de análisis y monitoreo ONE IT, dos de las cuales están clasificadas como críticas en cuanto a su gravedad.

La lista de vulnerabilidades es la siguiente:

- Con una puntuación CVSS de 9,9: una falla no especificada que puede ser aprovechada por un usuario no autenticado para obtener información sobre la conexión del servidor SQL que Veeam ONE utiliza para acceder a su base de datos de configuración, lo que resulta en la ejecución remota de código en el servidor SQL.
- Con una puntuación CVSS de 9,8: una falla en Veeam ONE que permite a un usuario sin privilegios con acceso al cliente web Veeam ONE obtener el hash NTLM de la cuenta utilizada por Veeam ONE Reporting Service.
- Con una puntuación CVSS de 4,5: una vulnerabilidad de secuencias de comandos entre sitios (XSS) que permite a un usuario con el rol Veeam ONE Power User obtener el token de acceso de un usuario con el rol Veeam ONE Administrator.
- Con una puntuación CVSS de: 4,3: una vulnerabilidad en Veeam ONE que permite a un usuario con el rol de usuario de solo lectura de Veeam ONE ver la programación del panel.

Si bien las primeras tres vulnerabilidades afectan las versiones 11, 11a, 12 de Veeam ONE, la última listada afecta solo a Veeam ONE 12. Las soluciones para los problemas están disponibles en las siguientes versiones:

- Veeam UNO 11 (11.0.0.1379)
- Veeam ONE 11a (11.0.1.1880)
- Veeam UNO 12 P20230314 (12.0.1.2591)

En los últimos meses, múltiples actores de amenazas, incluidos FIN7 y BlackCat ransomware, han aprovechado fallas críticas en el software de respaldo de Veeam para distribuir malware.

Remediación / Referencias

Se recomienda a los usuarios que ejecutan las versiones afectadas que detengan los servicios de monitoreo e informes de Veeam ONE, reemplacen los archivos existentes con los archivos proporcionados en la revisión y reinicien los dos servicios.

Por mayor información acceder a:

https://thehackernews.com/2023/11/critical-flaws-discovered-in-veeam-one.html

Malware BlazeStealer en Paquetes Python

CRÍTICO

Descripción

Advertencia, desarrolladores: malware BlazeStealer descubierto en paquetes Python en PyPI.

Estado

Un nuevo conjunto de paquetes Python maliciosos se ha abierto camino hasta el repositorio del Índice de paquetes Python (PyPI) con el objetivo final de robar información confidencial de los sistemas de desarrollo comprometidos.

Los paquetes se hacen pasar por herramientas de ofuscación aparentemente inofensivas, pero albergan un malware llamado BlazeStealer, informaron los investigadores.

BlazeStealer recupera un script malicioso adicional de una fuente externa, habilitando un bot de Discord que brinda a los atacantes control total sobre la computadora de la víctima.

La campaña, que comenzó en enero de 2023, incluye un total de ocho paquetes denominados Pyobftoexe, Pyobfusfile, Pyobfexecute, Pyobfpremium, Pyobflite, Pyobfadvance, Pyobfuse y pyobfgood, el último de los cuales se publicó en octubre.

Estos módulos vienen con archivos setup.py e init.py que están diseñados para recuperar un script de Python alojado en transfer[.]sh, que se ejecuta inmediatamente después de su instalación.

Llamado BlazeStealer, el malware ejecuta un bot de Discord y permite al actor de amenazas recopilar una amplia gama de información, incluidas contraseñas de navegadores web y capturas de pantalla, ejecutar comandos arbitrarios, cifrar archivos y desactivar Microsoft Defender Antivirus en el host infectado. Es más, puede inutilizar la computadora aumentando el uso de la CPU, insertando un script de Windows Batch en el directorio de inicio para apagar la máquina e incluso forzando un error de pantalla azul de la muerte (BSoD).

Es lógico que los desarrolladores involucrados en la ofuscación de código probablemente estén tratando con información valiosa y sensible y, por lo tanto, para un hacker, esto se traduce en un objetivo que vale la pena perseguir.

La mayoría de las descargas asociadas con los paquetes maliciosos se originaron en los EE. UU., seguidos de China, Rusia, Irlanda, Hong Kong, Croacia, Francia y España. Se descargaron colectivamente 2.438 veces antes de ser eliminados.

El dominio de código abierto sigue siendo un terreno fértil para la innovación, pero exige precaución. Los desarrolladores deben permanecer atentos y examinar los paquetes antes de su consumo.

El desarrollo se produce cuando la empresa de seguridad de la cadena de suministro de software Phylum descubrió una colección de módulos npm con temas criptográficos (puma-com, erc20-testenv, blockledger, cryptotransact y chainflow) con capacidades para entregar sigilosamente un malware de siguiente etapa.

En los últimos años, los repositorios de código abierto se han convertido en una forma lucrativa para que los actores de amenazas propaguen malware. Según el Informe de seguridad de la cadena de suministro de software sobre la evolución de Phylum para el tercer trimestre de 2023, se encontró que 13,708 paquetes en múltiples ecosistemas ejecutaban código sospechoso durante la instalación.

"1.481 paquetes descargaron y ejecutaron código subrepticiamente desde una fuente remota", informó la compañía el mes pasado. "10,201 paquetes hacían referencia a URL maliciosas conocidas, y se identificaron 2,598 paquetes typosquat".

Remediación / Referencias

Por mayor información acceder a: https://thehackernews.com/2023/11/beware-developers-blazestealer-malware.html

Microsoft Azure	Descubren Minero de Criptomonedas indetectable en Azure Automation	CRÍTICO

Descripción

Investigadores descubren una técnica de criptominería indetectable en Azure Automation

Estado

Investigadores de ciberseguridad han desarrollado lo que es el primer minero de criptomonedas basado en la nube totalmente indetectable que aprovecha el servicio Microsoft Azure Automation sin acumular ningún cargo.

Los investigadores descubrieron tres métodos diferentes para ejecutar el minero, incluido uno que puede ejecutarse en el entorno de la víctima sin llamar la atención.

Si bien esta investigación es importante debido a su impacto potencial en la minería de criptomonedas, también creemos que tiene serias implicaciones para otras áreas, ya que las técnicas podrían usarse para lograr cualquier tarea que requiera la ejecución de código en Azure.

El estudio se propuso principalmente identificar un "criptominero definitivo" que ofrezca acceso ilimitado a recursos computacionales, al mismo tiempo que requiera poco o ningún mantenimiento, sea gratuito e indetectable.

Ahí es donde entra en juego Azure Automation. Desarrollado por Microsoft, es un servicio de automatización basado en la nube que permite a los usuarios automatizar la creación, implementación, monitoreo y mantenimiento de recursos en Azure.

Se encontró un error en la calculadora de precios de Azure que permitía ejecutar una cantidad infinita de trabajos de forma totalmente gratuita, aunque se relaciona con el entorno del atacante en sí. Desde entonces, Microsoft ha publicado una solución para el problema.

Un método alternativo implica crear un trabajo de prueba para minería, luego establecer su estado como "Error" y luego crear otro trabajo de prueba ficticio aprovechando el hecho de que solo se puede ejecutar una prueba al mismo tiempo.

El resultado final de este flujo es que oculta completamente la ejecución de código dentro del entorno de Azure.

Un actor de amenazas podría aprovechar estos métodos estableciendo un shell inverso hacia un servidor externo y autenticándose en el punto final de automatización para lograr sus objetivos.

Además, se descubrió que la ejecución del código se podría lograr aprovechando la función de Azure Automation que permite a los usuarios cargar paquetes Python personalizados.

"Podríamos crear un paquete malicioso llamado 'pip' y cargarlo en la cuenta de automatización", explicaron investigadores. "El flujo de carga reemplazaría el pip actual en la cuenta de Automatización. Después de guardar nuestro pip personalizado en la cuenta de Automatización, el servicio lo usó cada vez que se cargó un paquete".

El grupo investigador también ha puesto a disposición una prueba de concepto denominada CloudMiner que está diseñada para obtener potencia informática gratuita dentro del servicio Azure Automation mediante el uso del mecanismo de carga de paquetes Python.

Microsoft, en respuesta a las revelaciones, ha caracterizado el comportamiento como "por diseño", lo que significa que el método aún puede explotarse sin que se le cobre.

Si bien el alcance de la investigación se limita al abuso de Azure Automation para la minería de criptomonedas, la firma de ciberseguridad advirtió que los actores de amenazas podrían reutilizar las mismas técnicas para lograr cualquier tarea que requiera la ejecución de código en Azure.

Como clientes proveedores de nube, las organizaciones individuales deben monitorear proactivamente cada recurso y cada acción que se realiza dentro de su entorno.

Remediación / Referencias

Recomendamos encarecidamente que las organizaciones se informen sobre los métodos y flujos que los actores maliciosos pueden utilizar para crear recursos indetectables y monitorear proactivamente la ejecución de código indicativo de dicho comportamiento.

Por mayor información acceder a:

https://thehackernews.com/2023/11/researchers-uncover-undetectable-crypto.html

	Alerta CISA: Explotación Activa de Vulnerabilidad SLP de Alta Gravedad"	CRÍTICO

Descripción

CISA: Vulnerabilidad SLP de alta gravedad ahora bajo explotación activa.

Estado

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) agregó el miércoles una falla de alta gravedad en el Protocolo de ubicación de servicios (SLP) a su catálogo de vulnerabilidades explotadas conocidas (KEV), citando evidencia de explotación activa.

Con una puntuación CVSS: 7.5 el problema se relaciona con una vulnerabilidad de denegación de servicio (DoS) que podría utilizarse como arma para lanzar ataques masivos de amplificación de DoS.

"El Protocolo de ubicación de servicios (SLP) contiene una vulnerabilidad de denegación de servicio (DoS) que podría permitir que un atacante remoto no autenticado registre servicios y utilice tráfico UDP falsificado para llevar a cabo un ataque de denegación de servicio (DoS) con un impacto significativo. factor de amplificación", dijo CISA.

SLP es un protocolo que permite que los sistemas de una red de área local (LAN) se descubran entre sí y establezcan comunicaciones.

Actualmente se desconocen los detalles exactos que rodean la naturaleza de la explotación de la falla, pero expertos advirtieron previamente que la deficiencia podría explotarse para realizar ataques DoS con un alto factor de amplificación.

"Este factor de amplificación extremadamente alto permite que un actor de amenazas con pocos recursos tenga un impacto significativo en una red y/o servidor objetivo a través de un ataque de amplificación DoS de reflexión", informaron.

Remediación / Referencias

A la luz de los ataques del mundo real que emplean la falla, las agencias federales deben aplicar las mitigaciones necesarias, incluida la desactivación del servicio SLP en sistemas que se ejecutan en redes que no son de confianza, antes del 29 de noviembre de 2023, para proteger sus redes contra posibles amenazas.

Por mayor información acceder a:

https://thehackernews.com/2023/11/cisa-alerts-high-severity-slp.html

Campaña Maliciosa: Sitio Falso de Noticias de Windows Distribuye Malware

CRÍTICO

Descripción

Nueva campaña de publicidad maliciosa utiliza un portal de noticias falso de Windows para distribuir instaladores maliciosos.

Estado

Se ha descubierto que una nueva campaña de publicidad maliciosa emplea sitios falsos que se hacen pasar por un portal legítimo de noticias de Windows para propagar un instalador malicioso de una popular herramienta de creación de perfiles del sistema llamada CPU-Z.

Este incidente es parte de una campaña de publicidad maliciosa más amplia que apunta a otras utilidades como Notepad++, Citrix y VNC Viewer, como se ve en su infraestructura (nombres de dominio) y plantillas de encubrimiento utilizadas para evitar la detección.

Si bien se sabe que las campañas de publicidad maliciosa crean sitios réplica que anuncian software ampliamente utilizado, la última actividad marca una desviación en el sentido de que el sitio web imita a WindowsReport[.]com.

El objetivo es engañar a los usuarios desprevenidos que buscan CPU-Z en motores de búsqueda como Google publicando anuncios maliciosos que, al hacer clic en ellos, los redireccionan al portal falso (workspace-app[.]online).

Al mismo tiempo, los usuarios que no son las víctimas previstas de la campaña reciben un blog inocuo con diferentes artículos, una técnica conocida como encubrimiento.

El instalador MSI firmado que está alojado en el sitio web fraudulento contiene un script de PowerShell malicioso, un cargador conocido como FakeBat (también conocido como EugenLoader), que sirve como conducto para implementar RedLine Stealer en el host comprometido.

Es posible que el actor de la amenaza haya elegido crear un sitio señuelo parecido a Windows Report porque muchas utilidades de software a menudo se descargan desde dichos portales en lugar de desde su página web oficial.

Esta no es la primera vez que los anuncios engañosos de Google para software popular resultan ser un vector de distribución de malware. Recientemente investigadores revelaron detalles de una campaña actualizada de Nitrogen que allana el camino para un ataque de ransomware BlackCat.

Otras dos campañas documentadas por expertos muestran que el método de descarga automática para dirigir a los usuarios a sitios web dudosos se ha aprovechado para

propagar varias familias de malware como NetWire RAT, DarkGate y DanaBot en los últimos meses.

El desarrollo se produce cuando los actores de amenazas continúan confiando cada vez más en kits de phishing de adversario en el medio (AiTM), como NakedPages, Strox y DadSec para eludir la autenticación multifactor y secuestrar cuentas específicas.

Para colmo, eSentire también llamó la atención sobre un nuevo método denominado ataque Wiki-Slack, un ataque dirigido al usuario que tiene como objetivo llevar a las víctimas a un sitio web controlado por el atacante desfigurando el final del primer párrafo de un artículo de Wikipedia y compartiendo en Slack.

Específicamente, explota una peculiaridad en Slack que "maneja mal el espacio en blanco entre el primer y segundo párrafo" para generar automáticamente un enlace cuando la URL de Wikipedia se presenta como una vista previa en la plataforma de mensajería empresarial.

Vale la pena señalar que un requisito previo clave para llevar a cabo este ataque es que la primera palabra del segundo párrafo del artículo de Wikipedia debe ser un dominio de nivel superior (por ejemplo, in, at, com o net) y que los dos párrafos deben aparecer dentro de las primeras 100 palabras del artículo.

Con estas restricciones, una amenaza podría convertir este comportamiento en un arma, de modo que la forma en que Slack formatea los resultados de vista previa de la página compartida apunte a un enlace malicioso que, al hacer clic, lleva a la víctima a un sitio con trampas explosivas.

Si uno no tiene barreras éticas, puede aumentar la superficie de ataque del ataque Wiki-Slack editando páginas de interés de Wikipedia para desfigurarlas.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/11/new-malvertising-campaign-uses-fake.html

SysAid®	Alerta de Día Cero: Lace Tempest Explota Vulnerabilidad en Software SysAid	CRÍTICO

Descripción

Alerta de día cero: Lace Tempest aprovecha la vulnerabilidad del software de soporte de TI SysAid.

Estado

El actor de amenazas conocido como Lace Tempest ha sido vinculado a la explotación de una falla de día cero en el software de soporte de TI SysAid en ataques limitados, según nuevos hallazgos de Microsoft.

Lace Tempest, conocido por distribuir el ransomware Cl0p, en el pasado aprovechó fallas de día cero en los servidores MOVEit Transfer y PaperCut.

Refiere a una falla de recorrido de ruta que podría resultar en la ejecución de código dentro de instalaciones locales. SysAid lo parchó en la versión 23.3.36 del software.

"Después de explotar la vulnerabilidad, Lace Tempest emitió comandos a través del software SysAid para entregar un cargador de malware para el malware Gracewire", dijo Microsoft.

"A esto normalmente le sigue la actividad operada por humanos, incluido el movimiento lateral, el robo de datos y la implementación de ransomware".

Según SysAid, se ha observado al actor de amenazas cargando un archivo WAR que contiene un shell web y otras cargas útiles en la raíz web del servicio web SysAid Tomcat.

El web shell, además de proporcionar al actor de la amenaza acceso por puerta trasera al host comprometido, se utiliza para entregar un script de PowerShell diseñado para ejecutar un cargador que, a su vez, carga Gracewire.

Los atacantes también implementaron un segundo script de PowerShell que se utiliza para borrar la evidencia de la explotación después de que se implementaron las cargas maliciosas.

Además, las cadenas de ataque se caracterizan por el uso del Agente MeshCentral y PowerShell para descargar y ejecutar Cobalt Strike, un marco legítimo post-explotación.

Se recomienda encarecidamente a las organizaciones que utilizan SysAid que apliquen los parches lo antes posible para frustrar posibles ataques de ransomware, así como escanear sus entornos en busca de signos de explotación antes de aplicar el parche.

El desarrollo se produce cuando la Oficina Federal de Investigaciones (FBI) de EE. UU. advirtió que los atacantes de ransomware tienen como objetivo proveedores externos y herramientas de sistemas legítimas para comprometer las empresas.

"A partir de junio de 2023, Silent Ransom Group (SRG), también llamado Luna Moth, llevó a cabo ataques de extorsión y robo de datos de phishing con devolución de llamada enviando a las víctimas un número de teléfono en un intento de phishing, generalmente relacionado con cargos pendientes en la cuenta de las víctimas". dijo el FBI.

Si una víctima cae en la trampa y llama al número de teléfono proporcionado, los actores maliciosos les indican que instalen una herramienta legítima de administración del sistema a través de un enlace proporcionado en un correo electrónico de seguimiento".

Luego, los atacantes utilizaron la herramienta de administración para instalar otro software auténtico que puede reutilizarse para actividades maliciosas, señaló la agencia,

agregando que los actores comprometieron archivos locales y unidades compartidas de red, exfiltraron datos de las víctimas y extorsionaron a las empresas.

Remediación / Referencias

Por mayor información acceder a:

https://thehackernews.com/2023/11/zero-day-alert-lace-tempest-exploits.html

Conclusiones

Las noticias recientes en ciberseguridad destacan la creciente complejidad y diversidad de amenazas en el panorama digital. Desde vulnerabilidades críticas en plataformas de monitoreo hasta la infiltración de malware en repositorios de paquetes Python, queda claro que la vigilancia constante y la rápida aplicación de parches son cruciales para mantener la seguridad informática.

La detección de un minero de criptomonedas indetectable en Azure Automation subraya la importancia de la monitorización proactiva de entornos en la nube y la necesidad de abordar posibles vectores de ataque. Las advertencias de la CISA sobre la explotación activa de vulnerabilidades, como en el caso del Protocolo de Ubicación de Servicios (SLP), resaltan la urgencia de aplicar mitigaciones y proteger las redes contra posibles amenazas.

La campaña maliciosa que utiliza sitios falsos de noticias de Windows como cebo subraya la sofisticación de los ataques publicitarios y la importancia de verificar la autenticidad de los sitios web al descargar software popular.

Finalmente, la identificación de un actor de amenazas vinculado a la explotación de una vulnerabilidad de día cero en el software de soporte de TI SysAid destaca la necesidad de que las organizaciones estén al tanto de las amenazas emergentes y apliquen rápidamente las actualizaciones de seguridad.

En conjunto, estas noticias subrayan la importancia de la educación continua en ciberseguridad, la implementación de mejores prácticas en desarrollo de software, la monitorización constante de entornos en la nube y la colaboración entre la comunidad de seguridad para abordar los desafíos en evolución del panorama cibernético.

Desde el equipo de Datasec seguimos protegiendo la seguridad de nuestros clientes, socios y colaboradores.

¡Hasta la próxima!