Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ARCANEDOOR: CIBERCRIMINALES APROVECHAN VULNERABILIDADES ZERO-DAY EN DISPOSITIVOS CISCO ASA

25/ 04 / 2024

CONTENIDO

INTRODUCCIÓN

En el mundo de la ciberseguridad, un nuevo y preocupante descubrimiento ha sacudido a las empresas y expertos del sector. Una campaña de malware conocida como ArcaneDoor ha explotado dos vulnerabilidades Zero-Day en dispositivos Cisco Adaptive Security Appliances (ASA), permitiendo a actores maliciosos obtener acceso no autorizado, modificar configuraciones y exfiltrar datos críticos. Con las amenazas a la seguridad de red en aumento, esta campaña destaca la importancia de mantener los dispositivos perimetrales seguros y actualizados para proteger la integridad de las redes corporativas y la información confidencial de los usuarios.

ARCANEDOOR: CIBERCRIMINALES APROVECHAN VULNERABILIDADES ZERO-DAY EN DISPOSITIVOS CISCO ASA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_04_25_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	25/04/2024
Es día cero (0 day):	No

RESUMEN

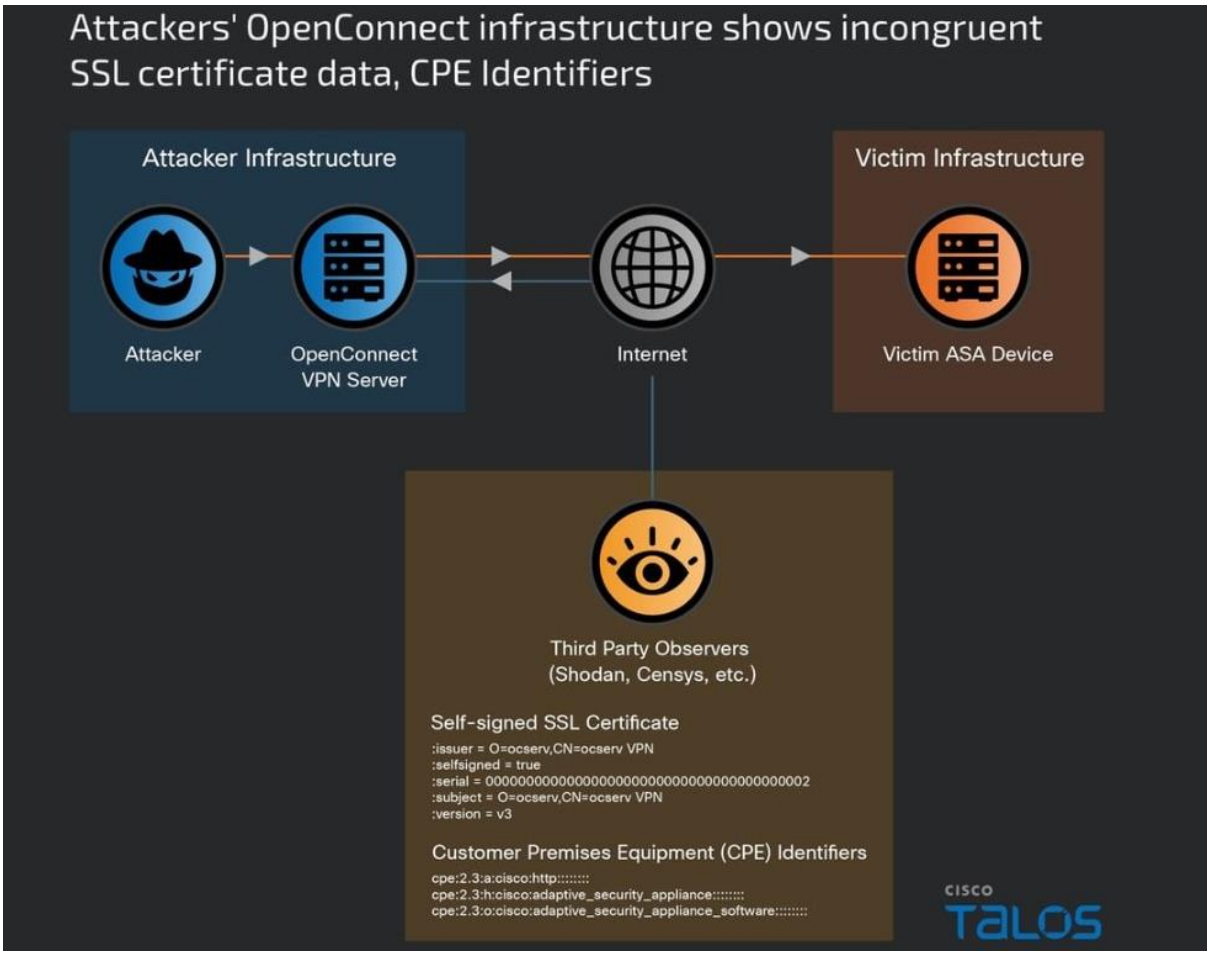
La comunidad de ciberseguridad ha sido sacudida por la noticia de una sofisticada campaña de malware que explota dos vulnerabilidades Zero-Day en equipos de red Cisco Adaptive Security Appliances (ASA). Denominada ArcaneDoor, esta campaña ha sido atribuidas a un grupo respaldado por el Estado y sin documentación previa, denominado UAT4356 o Storm-1849 por Microsoft.

Puertas Traseras Peligrosas y Amenazas Latentes

El equipo de seguridad Cisco Talos descubrió que UAT4356 implementó dos puertas traseras como parte de esta campaña: "Line Runner" y "Line Dancer". Estos implantes permitieron acciones maliciosas como modificación de configuraciones, reconocimiento, captura y exfiltración de tráfico de red, y potencialmente movimiento lateral dentro de las redes afectadas.

CVE-2024-20353: Vulnerabilidad de denegación de servicio en los servicios web de Cisco ASA y Firepower Threat Defense, con una puntuación CVSS de 8,6.

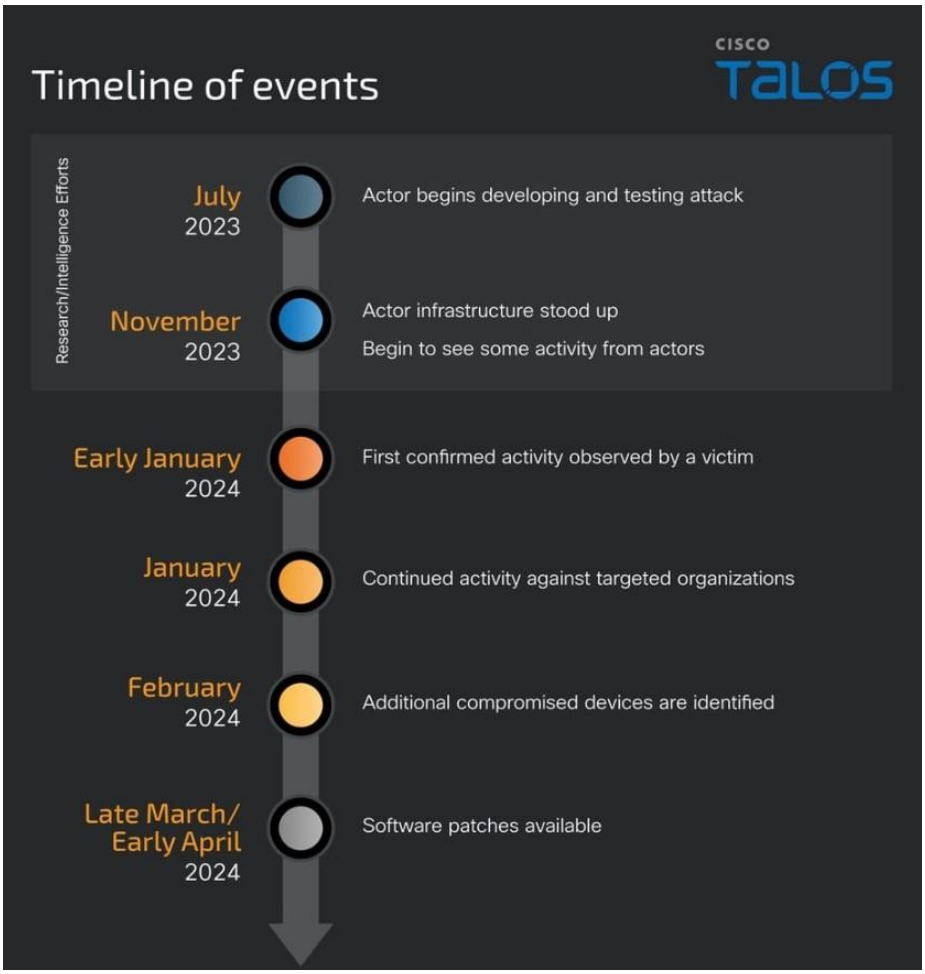
CVE-2024-20359: Vulnerabilidad de ejecución persistente de código local en el software de Cisco ASA y Firepower Threat Defense, con una puntuación CVSS de 6,0. Esta vulnerabilidad permite a un atacante local ejecutar código arbitrario con privilegios de nivel root.



Campaña Bien Planificada y Persistente

Lo que hace única a esta campaña es la meticulosa atención del grupo para ocultar sus huellas y la capacidad de emplear métodos avanzados para evadir el análisis forense en memoria. Los actores parecen tener una comprensión completa del funcionamiento interno de ASA y las acciones forenses comunes que utiliza Cisco para validar la integridad de los dispositivos de red.

En cuanto a la ruta de acceso inicial utilizada para violar los dispositivos, aún se desconoce, pero se dice que UAT4356 comenzó los preparativos para ello desde julio de 2023. Un punto de apoyo exitoso fue seguido por el despliegue de los implantes "Line Dancer" y "Line Runner", donde este último es una puerta trasera basada en HTTP que puede persistir a través de reinicios y actualizaciones.



Riesgo para la Seguridad de Redes Perimetrales

El incidente destaca el creciente interés de los cibercriminales por atacar dispositivos perimetrales como servidores de correo electrónico, firewalls y VPN, que históricamente carecen de soluciones de detección y respuesta de endpoints (EDR). Cisco Talos no especificó cuántos clientes fueron comprometidos, pero se ha observado que tanto grupos cibernéticos respaldados por China como por Rusia han atacado dispositivos de red Cisco para ciberespionaje en el pasado.

Medidas de Mitigación y Recomendaciones

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU. (CISA) agregó las fallas a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), exigiendo a las agencias federales que apliquen las correcciones proporcionadas por los proveedores antes del 1 de mayo de 2024.

Para mitigar el riesgo de estos ataques, es fundamental aplicar las siguientes medidas:

- Parches Rutinarios: Asegúrese de mantener los dispositivos de red perimetral actualizados con los últimos parches de seguridad.
- Monitoreo Constante: Implemente un sistema de monitoreo y alerta para detectar actividad sospechosa en los dispositivos de red.
- Pruebas de Vulnerabilidades: Realice pruebas de vulnerabilidad y auditorías de seguridad regularmente para detectar posibles puntos débiles.
- Los ataques dirigidos a dispositivos perimetrales siguen siendo una amenaza persistente, y es crucial para las organizaciones adoptar un enfoque proactivo para proteger sus redes contra estos sofisticados ataques.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240425_1_ArcaneDoor

NOTICIA COMPLETA

https://devel.group/blog/arcanedoor-cibercriminales-aprovechan-vulnerabilidades-zero-day-en-dispositivos-cisco-asa/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente