Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ATAQUES CON IA DE HEXSTRIKE EXPLOTAN FALLAS DE CITRIX UNA SEMANA DESPUÉS DE SU DIVULGACIÓN

04/ 09 / 2025

CONTENIDO

INTRODUCCIÓN

Un nuevo informe revela que HexStrike AI, un marco de seguridad ofensiva impulsado por inteligencia artificial ha sido adaptado por cibercriminales en menos de 12 horas desde su lanzamiento. Lo que fue creado para equipos de seguridad y red teaming ahora se está utilizando para explotar vulnerabilidades de Citrix NetScaler (CVE-2025-7775, CVE-2025-7776 y CVE-2025-8424), difuminando la línea entre la investigación legítima y el ciberdelito.

ATAQUES CON IA DE HEXSTRIKE EXPLOTAN FALLAS DE CITRIX UNA SEMANA DESPUÉS DE SU DIVULGACIÓN

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

ID de alerta:	DSOC-CERT_2025_09_04_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	04/09/2025
Es día cero (0 day):	No

RESUMEN

Un nuevo informe revela que HexStrike AI, un marco de seguridad ofensiva impulsado por inteligencia artificial ha sido adaptado por cibercriminales en menos de 12 horas desde su lanzamiento. Lo que fue creado para equipos de seguridad y red teaming ahora se está utilizando para explotar vulnerabilidades de Citrix NetScaler (CVE-2025-7775, CVE-2025-7776 y CVE-2025-8424), difuminando la línea entre la investigación legítima y el ciberdelito.

¿Cómo funciona la herramienta?

HexStrike AI funciona como un cerebro de IA que orquesta módulos de ataque de forma autónoma. Su poder reside en su capacidad para automatizar tareas que antes eran manuales:

- Escaneo de objetivos: Identifica automáticamente sistemas potencialmente vulnerables en internet.
- Generación de exploits: Utiliza modelos de lenguaje avanzados (LLMs) para generar exploits de manera dinámica, basándose en la descripción de los CVEs y el código disponible públicamente.
- Persistencia: Entrega la carga útil (payload) y establece la persistencia en el sistema, ajustando la técnica si el primer intento falla.
- Evasión adaptativa: La IA reescribe sus propios métodos en tiempo real para evadir la detección.

Este nivel de automatización significa que lo que antes requería días o semanas de trabajo manual, ahora puede ejecutarse en cuestión de minutos y a gran escala.

Implicaciones de la amenaza

La aparición de HexStrike AI tiene consecuencias preocupantes para la ciberseguridad global:

- Ventana de parcheo nula: Antes, las organizaciones tenían un margen de tiempo para aplicar los parches después de que se divulgaba un CVE. Con esta herramienta, la explotación puede ocurrir casi de inmediato, reduciendo la ventana de protección a cero.
- Escenario geopolítico: Expertos alertan que grupos patrocinados por Estados-nación podrían aprovechar frameworks de IA como HexStrike para campañas de espionaje o sabotaje digital masivo.
- Desafío para los defensores: Las soluciones tradicionales basadas en firmas ya no son suficientes. Se requieren defensas automatizadas y adaptativas que puedan identificar comportamientos anómalos.

RECOMENDACIONES

- Aplica los parches de Citrix NetScaler de inmediato para mitigar las vulnerabilidades CVE-2025-7775, CVE-2025-7776 y CVE-2025-8424.
- Implementa detección basada en comportamiento (EDR/NDR) que pueda identificar patrones anómalos, más allá de las firmas tradicionales.
- Automatiza tu defensa adoptando sistemas SOAR y de respuesta rápida para contrarrestar ataques a gran escala.
- Monitorea la inteligencia de amenazas para detectar cualquier actividad relacionada con HexStrike AI en la dark web.

NOTICIA COMPLETA

https://devel.group/blog/ataques-con-ia-de-hexstrike-explotan-fallas-de-citrix-una-semana-despues-de-su-divulgacion/

CONTACTOS DE SOPORTE

Correo electrónico: cti@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://devel.group