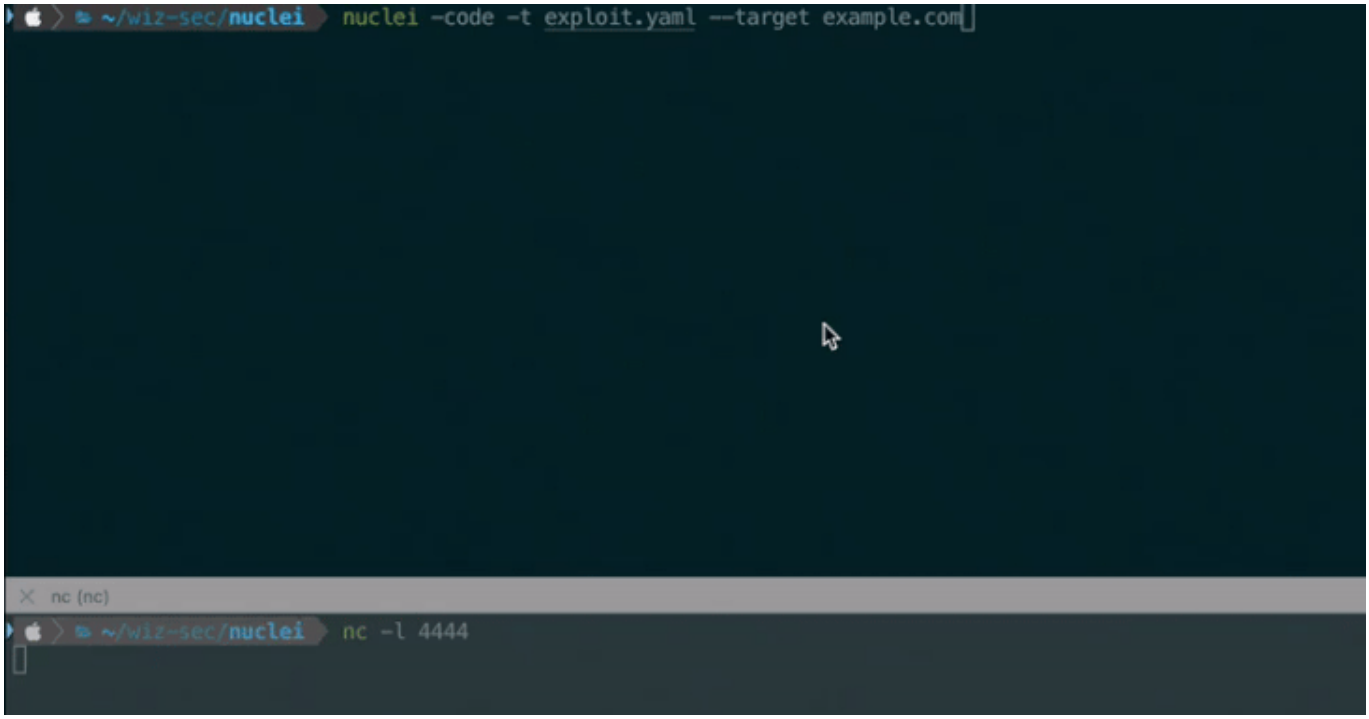
Se ha descubierto una vulnerabilidad crítica en Nuclei, el escáner de vulnerabilidades de código abierto desarrollado por ProjectDiscovery. Esta falla podría permitir a los atacantes eludir la verificación de firmas y ejecutar código malicioso si es aprovechada de manera exitosa.

Catalogada como CVE-2024-43405, tiene una puntuación CVSS de 7.4 sobre 10 y afecta a todas las versiones posteriores a la 3.0.0 de Nuclei.



> *«El problema surge debido a una discrepancia en cómo el proceso de verificación de firmas y el analizador YAML manejan los caracteres de salto de línea, combinado con el tratamiento de múltiples firmas,»* señala la descripción de la vulnerabilidad.
>
> *«Esto da lugar a que un atacante pueda inyectar contenido malicioso en una plantilla, manteniendo una firma válida para la parte legítima de la plantilla.»*

Nuclei es una herramienta diseñada para detectar vulnerabilidades en aplicaciones modernas, infraestructuras, entornos en la nube y redes. Su motor de escaneo se basa en plantillas, que son archivos YAML, para enviar solicitudes específicas y así identificar posibles fallas de seguridad.

También tiene la capacidad de ejecutar código externo en el sistema operativo del host mediante el protocolo code, lo que brinda a los investigadores una mayor flexibilidad en las pruebas de seguridad.

La compañía de seguridad en la nube Wiz, que identificó la vulnerabilidad CVE-2024-43405, explicó que la falla radica en el proceso de verificación de firmas de las plantillas. Este proceso asegura la integridad de las plantillas oficiales disponibles en el repositorio.

Si esta vulnerabilidad es explotada, los atacantes podrían evitar este paso crucial de verificación, lo que les permitiría crear plantillas maliciosas capaces de ejecutar código arbitrario y obtener acceso a datos sensibles en el sistema.

> *«Actualmente, la verificación de firmas es el único mecanismo que existe para validar las plantillas de Nuclei, lo que convierte esta falla en un posible punto único de fallo,»* dijo Guy Goldenberg, investigador de Wiz, en un análisis reciente.

El núcleo del problema está en el uso de expresiones regulares (regex) para validar las firmas, combinado con conflictos en el análisis que surgen al emplear regex y YAML juntos. Esto permite que un atacante introduzca un carácter `\r`, el cual evade la verificación basada en regex pero es tratado como un salto de línea por el analizador YAML.

En otras palabras, estas inconsistencias en el análisis pueden explotarse para crear una plantilla de Nuclei que incluya un carácter `\r` y una segunda línea `# digest:` que no sea detectada durante la verificación, pero sí interpretada y ejecutada por el analizador YAML.

> *«El sistema de validación basado en regex de Go considera `\r` como parte de la misma línea, mientras que el analizador YAML lo interpreta como un salto de línea. Este comportamiento inconsistente permite que los atacantes inserten contenido que pase la verificación pero sea ejecutado por el analizador YAML,»* explicó Goldenberg.
>
> *«Además, el proceso de verificación de firmas omite intencionadamente la línea de firma del contenido de la plantilla, pero solo valida la primera línea, dejando las demás sin verificar pero ejecutables.»*

Tras el reporte responsable de la vulnerabilidad, ProjectDiscovery solucionó el problema el 4 de septiembre de 2024 en la versión 3.3.2. La última versión de Nuclei actualmente es la 3.3.7.

> *«Los atacantes podrían diseñar plantillas maliciosas con líneas manipuladas `# digest` o incluir saltos de línea `\r` de forma estratégica para superar la verificación de firmas de Nuclei,»* comentó Goldenberg.
>
> *«Este riesgo se incrementa cuando las organizaciones ejecutan plantillas no verificadas o provenientes de la comunidad sin realizar una validación o aislamiento adecuado. Un atacante podría aprovechar esta funcionalidad para introducir plantillas maliciosas, lo que podría dar lugar a la ejecución arbitraria de comandos, robo de datos o la vulneración del sistema.»*