Se han dado a conocer múltiples deficiencias de seguridad en el software de monitoreo de redes Nagios XI que podrían conllevar a la elevación de privilegios y la divulgación de información.

Los cuatro agujeros de seguridad, identificados desde CVE-2023-40931 hasta CVE-2023-40934, afectan a las versiones de Nagios XI 5.11.1 y versiones anteriores. Tras una divulgación responsable el 4 de agosto de 2023, se han solucionado a partir del 11 de septiembre de 2023, con el lanzamiento de la versión 5.11.2.

> Según la investigadora de Outpost24, Astrid Tedenbrant, *«Tres de estas vulnerabilidades (CVE-2023-40931, CVE-2023-40933 y CVE-2023-40934) permiten a los usuarios, con diversos niveles de privilegios, acceder a campos de la base de datos a través de inyecciones SQL.»*

> *«La información obtenida a raíz de estas vulnerabilidades puede utilizarse para aumentar los privilegios en el producto y obtener datos confidenciales de usuarios, como contraseñas cifradas y tokens de API.»*

Por otro lado, CVE-2023-40932 está relacionado con un defecto de scripting entre sitios (XSS) en el componente de Logotipo Personalizado que podría emplearse para leer información sensible, incluyendo contraseñas en texto plano desde la página de inicio de sesión.

A continuación, se detalla la lista de fallos:

- CVE-2023-40931 – Inyección SQL en el punto de reconocimiento de banner
- CVE-2023-40932 – Scripting entre sitios en el componente de Logotipo Personalizado.
- CVE-2023-40933 – Inyección SQL en la configuración de banner de anuncios.
- CVE-2023-40934 – Inyección SQL en la Escalada de Host/Servicio en el Administrador de Configuración Principal (CCM).

La explotación exitosa de las tres vulnerabilidades de inyección SQL podría permitir que un atacante autenticado ejecute comandos SQL arbitrarios, mientras que el fallo XSS podría ser aprovechado para inyectar código JavaScript arbitrario y acceder y modificar datos de la página.

Esta no es la primera vez que se descubren problemas de seguridad en Nagios XI. En 2021, Skylight Cyber y Claroty descubrieron hasta dos docenas de deficiencias que podrían ser utilizadas para tomar el control de la infraestructura y lograr la ejecución de código de forma remota.