BOLETÍN DE ALERTA

Boletín Nro.: 2023-02
Fecha de publicación: 22/08/2023
Tema: Vulnerabilidades críticas en productos Nagios
Traffic Light Protocol (TLP): White

Producto afectado:

- Nagios XI en sus versiones 5.11.1 y anteriores.

Descripción:

Se han *reportado* vulnerabilidades críticas de tipo Inyección SQL que afectan al software de monitoreo de red Nagios XI, que podrían resultar en escalación de privilegios.

La lista de vulnerabilidades se describe a continuación:

- CVE-2023-40933 - SQL Injection en la configuración del banner de anuncio con criticidad Alta con puntaje 8.8, permite a atacantes autenticados con privilegios de configuración de banners de anuncios ejecutar comandos SQL arbitrarios a través del parámetro ID enviado a la función update_banner_message().

- CVE-2023-40934 - SQL Injection en la escalación de host/servicio en Core Configuration Manager (CCM) con criticidad Alta con puntaje 7.2.

- CVE-2023-40931 - Inyección SQL en banner que reconoce el punto final con criticidad Media con puntaje 6.5. Permite a atacantes autenticados ejecutar comandos SQL arbitrarios a través del parámetro ID en la solicitud POST a /nagiosxi/admin/banner_message-ajaxhelper.php

- CVE-2023-40932 - Cross-Site Scripting en el componente de logotipo personalizado con criticidad Media con puntaje 5.4. Permite a los atacantes autenticados con acceso al componente del logotipo personalizado inyectar javascript o HTML de su elección a través del campo de texto alternativo. Esto afecta a todas las páginas que contienen la barra de navegación, incluida la página de inicio de sesión, lo que significa que el atacante puede robar credenciales de texto sin formato.

Impacto:
La explotación exitosa de las estas vulnerabilidades podría permitir a un atacante autenticado obtener información de la base de datos vinculada a Nagios y, por tanto, obtener datos sensibles, incluido credenciales válidas

Prevención:
El equipo de Nagiox XI ha lanzado un parche que soluciona las vulnerabilidades mencionadas. Se recomienda aplicar el parche lo antes posible. Enlace de descarga *aquí*.

- *Nagios XI versión 5.11.2* o posterior.

Información adicional:

- *https://thehackernews.com/2023/09/critical-security-flaws-exposed-in.html*
- *https://outpost24.com/blog/nagios-xi-vulnerabilities/*
- https://www.nagios.com/products/security/