



NCSC-2025-0065

Kwetsbaarheden verholpen in Nagios XI

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 21-02-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Nagios heeft kwetsbaarheden verholpen in Nagios XI (Specifiek voor versie 2024R1.2.2).

Duiding

De kwetsbaarheid bevindt zich in de manier waarop Nagios XI omgaat met gebruikersinformatie, waardoor niet-geauthenticeerde gebruikers toegang kunnen krijgen tot gebruikersnamen en e-mailadressen van alle huidige gebruikers. Dit kan leiden tot ongeautoriseerde toegang en exploitatie van gebruikersdata. Daarnaast is er een SQL-injectie kwetsbaarheid aanwezig in de History Tab component, waarmee kwaadwillenden op afstand willekeurige SQL-commando's kunnen uitvoeren door middel van speciaal vervaardigde payloads.

Oplossingen

Nagios heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://github.com/advisories/GHSA-4cmp-m2j4-4727>
- <https://github.com/advisories/GHSA-39j3-r3vp-hgfh>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-54961	6.5 MEDIUM
➤ CVE-2024-54960	5.3 MEDIUM

CWE's

CWE	Beschrijving
➤ CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
➤ CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

Getroffen producten

nagios_enterprises
nagios_xi
nagios
nagios_xi

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.