Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0349

Kwetsbaarheden verholpen in Nagios XI

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 03-11-2025

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 (Versies voor 2024R1.4.2 en 2024R2).

Duiding

De kwetsbaarheden omvatten een remote code execution kwetsbaarheid binnen de Business Process Intelligence component, onvoldoende permissies op systemd unit bestanden, ongeautoriseerde toegang tot API-sleutels, een command injection kwetsbaarheid in de WinRM plugin, en een kritieke remote code execution kwetsbaarheid in de Core Config Manager. Deze kwetsbaarheden kunnen worden misbruikt door geauthenticeerde gebruikers om willekeurige code uit te voeren, wat kan leiden tot een compromittering van de systeemintegriteit en de vertrouwelijkheid van gevoelige API-gegevens. De kwetsbaarheden benadrukken de noodzaak van robuuste validatiemechanismen en correcte toegangscontrole binnen de getroffen versies.

Oplossingen

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

Referenties

- https://www.nagios.com/products/security/#nagios-xi

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-34134	9.4 CRITICAL
CVE-2025-34135	5.1 MEDIUM
CVE-2025-34283	7.1 HIGH
CVE-2025-34284	9.4 CRITICAL
CVE-2025-34286	9.4 CRITICAL
CVE-2025-34287	8.4 HIGH

CWE's

CWE	Beschrijving
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-732	Incorrect Permission Assignment for Critical Resource

Getroffen producten

Nagios Enterprises
Nagios XI

Disclaimer