Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0200

Kwetsbaarheden verholpen in IBM QRadar SIEM

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 20-06-2025

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

IBM heeft kwetsbaarheden verholpen in IBM QRadar SIEM (Specifiek voor versie 7.5.0 Update Package 12).

Duiding

De kwetsbaarheden omvatten een mogelijkheid voor een bevoegde gebruiker om kritieke configuratiebestanden te wijzigen, wat kan leiden tot het uploaden van schadelijke autoupdatebestanden en het uitvoeren van willekeurige commando's binnen het systeem. Daarnaast is er een kwetsbaarheid gerelateerd aan een XML externe entiteit injectie (XXE) aanval, die kan leiden tot ongeautoriseerde toegang tot gevoelige informatie of uitputting van geheugbronnen. Ook kan gevoelige informatie worden opgeslagen in logbestanden die toegankelijk zijn voor lokale gebruikers, wat het risico op ongeautoriseerde gegevensblootstelling met zich meebrengt.

Oplossingen

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

Referenties

- https://www.ibm.com/support/pages/node/7237317

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-33117	8.6 HIGH
CVE-2025-33121	5.3 MEDIUM
CVE-2025-36050	4.8 MEDIUM

CWE's

CWE	Beschrijving
CWE-611	Improper Restriction of XML External Entity Reference

CWE-73	External Control of File Name or Path
CWE-532	Insertion of Sensitive Information into Log File

Getroffen producten

IBM
QRadar SIEM

Disclaimer