Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0141

Kwetsbaarheden verholpen in Keycloak

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 06-05-2025

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

Red Hat heeft kwetsbaarheden verholpen in Keycloak.

Duiding

De kwetsbaarheden omvatten een probleem waarbij JWT-tokens met lange vervaltijden kunnen leiden tot oneindige groei in de cache, wat kan resulteren in een OutOfMemoryError en een Denial-of-Service voor legitieme gebruikers. Daarnaast kan de verificatie van trust store-certificaten worden overgeslagen als het verificatiebeleid is ingesteld op 'ALL', wat kan leiden tot ongeautoriseerde toegang. Bovendien kan een kwetsbaarheid in het org.keycloak.authorization-pakket gebruikers in staat stellen om vereiste beveiligingsacties te omzeilen, zoals het inschakelen van twee-factor-authenticatie, wat de beveiliging van gebruikersaccounts in gevaar kan brengen.

Oplossingen

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

Referenties

- https://access.redhat.com/errata/RHSA-2025:4335
- https://access.redhat.com/hydra/rest/securitydata/csaf/RHSA-2025:4335.json
- https://access.redhat.com/errata/RHSA-2025:4336
- https://access.redhat.com/hydra/rest/securitydata/csaf/RHSA-2025:4336.json

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-2559	**6.9 MEDIUM**
CVE-2025-3501	**6.9 MEDIUM**
CVE-2025-3910	**6.9 MEDIUM**

CWE's

CWE	Beschrijving
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-287	Improper Authentication

Getroffen producten

Red Hat
Red Hat build of Keycloak 26.0
keycloak-rhel9
keycloak-rhel9-operator
org.keycloak.authentication
Open Source
Keycloak

Disclaimer