Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0326

Kwetsbaarheden verholpen in Keycloak

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 25-08-2026

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 meerdere kwetsbaarheden verholpen in Keycloak.

Duiding

De kwetsbaarheid met CVE-2026-18963 kan een ongeauthenticeerde externe aanvaller in staat stellen om elke gebruikersaccount over te nemen door een wachtwoordreset af te dwingen. Door deze kwetsbaarheid valt het e-mailverificatieproces bij wachtwoordreset te omzeilen en wachtwoorden van gebruikers te wijzigen.

In Keycloak zijn daarnaast kwetsbaarheden aanwezig in de Fine-Grained Admin Permissions (FGAP) v2, waardoor bepaalde beheerders met beperkte permissies metadata van verborgen groepen kunnen inzien en details van ongeautoriseerde oudergroepen kunnen blootstellen. Verder kunnen geauthenticeerde aanvallers via een legacy client-initiated account-linking endpoint CSRF-bescherming omzeilen en accounts overnemen. Ook kunnen gedelegeerde beheerders met alleen leesrechten client secrets uitlezen door een fout in de secret rotation. Voor OpenTelemetry Java was er een kwetsbaarheid waarbij het ontbreken van limieten op baggage headers leidde tot onbegrensd geheugen- en CPU-gebruik, wat Denial-of-Service kan veroorzaken. Bij Jackson-libraries is een bypass van de @JsonIgnore annotatie in Java Records vastgesteld, waardoor ongewenste toewijzing aan constructorparameters mogelijk is. Ook zijn er bypasses van @JsonIgnoreProperties, ontbrekende view guards op @JsonUnwrapped en ongeautoriseerde schrijfacties op velden met @JsonView. Oracle Database Server's Fleet Patching and Provisioning component is eveneens getroffen door een kwetsbaarheid die ongeautoriseerde data toegang of Denial-of-Service kan veroorzaken.

Oplossingen

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

Referenties

- https://access.redhat.com/errata/RHSA-2026:56519
- https://access.redhat.com/errata/RHSA-2026:56520
- https://access.redhat.com/errata/RHSA-2026:56523
- https://access.redhat.com/errata/RHSA-2026:56524
- https://www.keycloak.org/2026/08/keycloak-2672-released

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-14613	4.3 MEDIUM
CVE-2026-15571	7.3 HIGH
CVE-2026-15945	4.3 MEDIUM
CVE-2026-17048	5.5 MEDIUM
CVE-2026-18963	9.1 CRITICAL
CVE-2026-45292	7.5 HIGH
CVE-2026-59888	6.5 MEDIUM
CVE-2026-59889	8.1 HIGH

CWE's

CWE	Beschrijving
CWE-341	Predictable from Observable State
CWE-502	Deserialization of Untrusted Data
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-640	Weak Password Recovery Mechanism for Forgotten Password
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-863	Incorrect Authorization
CWE-915	Improperly Controlled Modification of Dynamically-Determined Object Attributes

Getroffen producten

Keycloak
keycloak
Red Hat
Build of Keycloak

Disclaimer