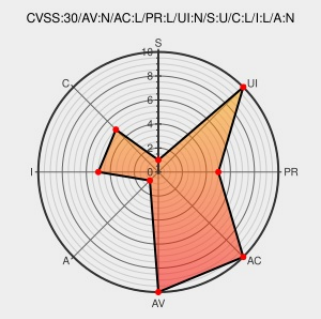
CVE-2018-10894

Published on: 08/01/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:21 PM UTC

CVE-2018-10894

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Enterprise Linux from Redhat contain the following vulnerability:

It was found that SAML authentication in Keycloak 3.4.3.Final incorrectly authenticated expired certificates. A malicious user could use this to access unauthorized data or possibly conduct further attacks.

CVE-2018-10894 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Red Hat** - **keycloak** version **3.4.3.Final**

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	LOW	NONE

CVSS2 Score: 5.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:3593

1599434 – (CVE-2018-10894) CVE-2018-10894 keycloak: auth permitted with expired certs in SAML client	Issue Tracking Patch Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10894
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:3592
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:3595
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2019:0877

Related QID Numbers

994825 Java (Maven) Security Update for org.keycloak:keycloak-core (GHSA-xvv8-8wh9-9fh2)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Keycloak	3.4.3	All	All	All
Application	Redhat	Keycloak	3.4.3	All	All	All
Application	Redhat	Single Sign-on	7.2	All	All	All
Application	Redhat	Single Sign-on	7.2	All	All	All

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:keycloak:3.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:keycloak:3.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:single_sign-on:7.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:single_sign-on:7.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→