CVE-2017-2585

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-2585
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-12 15:29:00 UTC
Updated	2018-04-12 15:14:00 UTC
Description	Red Hat Keycloak before version 2.5.1 has an implementation of HMAC verification for JWS tokens that uses a method tha

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Application	Redhat	Keycloak	All	All	All	All
Application	Redhat	Keycloak	All	All	All	All
Application	Redhat	Single Sign On	7.1	All	All	All
Application	Redhat	Single Sign On	7.2	All	All	All
Application	Redhat	Single Sign On	7.1	All	All	All
Application	Redhat	Single Sign On	7.2	All	All	All

References

Reference
1412376 – (CVE-2017-2585) CVE-2017-2585 keycloak: timing attack in JWS signature verification
Red Hat Customer Portal
Keycloak CVE-2017-2585 Security Bypass Vulnerability
Red Hat Customer Portal

Red Hat Single Sign-On Bugs Let Remote Authenticated Users Delete User Accounts in a Different Realm and Let Remote Users Obtain Pote
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980815 Java (maven) Security Update for org.keycloak:keycloak-core (GHSA-w6gv-3r3v-gwgj)