CVE-2020-25680

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

Summary

CVE	CVE-2020-25680
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-07 18:15:00 UTC
Updated	2021-01-14 17:01:00 UTC
Description	A flaw was found in JBCS httpd in version 2.4.37 SP3, where it uses a back-end worker SSL certificate with the keystore file

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Core Services Httpd	2.4.37	sp3	All	All
Application	Redhat	Jboss Core Services Httpd	2.4.37	sp3	All	All

References

Reference
1892703 – (CVE-2020-25680) CVE-2020-25680 httpd: allow connecting via SSL to a backend worker when the backend keystore file's ID is 'u
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**