CVE-2022-2256

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

Summary

CVE	CVE-2022-2256
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-01 21:15:00 UTC
Updated	2022-10-18 18:42:00 UTC
Description	A Stored Cross-site scripting (XSS) vulnerability was found in keycloak as shipped in Red Hat Single Sign-On 7. This flaw a

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Single Sign-on	7.0	All	All	All

References

Reference	Source	Link
github.com/keycloak/keycloak/security/advisories/GHSA-w9mf-83w3-fv49	MISC	github.com
2101942 – (CVE-2022-2256) CVE-2022-2256 keycloak: improper input validation permits script injection	MISC	bugzilla.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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**