CVE-2022-1274

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

Summary

CVE	CVE-2022-1274
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-29 21:15:00 UTC
Updated	2023-12-22 16:15:00 UTC
Description	A flaw was found in Keycloak in the execute-actions-email endpoint. This issue allows arbitrary HTML to be injected into em

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.0	All	All	All
Application	Redhat	Keycloak	All	All	All	All
Application	Redhat	Openshift Container Platform	4.10	All	All	All
Application	Redhat	Openshift Container Platform	4.9	All	All	All
Application	Redhat	Single Sign-on	All	All	All	All
Application	Redhat	Single Sign-on	-	All	All	All

References

Reference	Source	Link	Tags
Bug Access Denied	MISC	bugzilla.redhat.com	
HTML Injection in Keycloak Admin REST API · Advisory · keycloak/keycloak · GitHub	MISC	github.com	

usd-2021-0033 - usd HeroLab		herolab.usd.de	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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