CVE-2021-3827

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

Summary

CVE	CVE-2021-3827
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-23 16:15:00 UTC
Updated	2022-11-30 18:46:00 UTC
Description	A flaw was found in keycloak, where the default ECP binding flow allows other authentication flows to be bypassed. By expl

Risk And Classification

Problem Types: CWE-287

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	8.0	All	All	All
Application	Redhat	Keycloak	All	All	All	All
Application	Redhat	Openshift Container Platform	4.8	All	All	All
Application	Redhat	Openshift Container Platform	4.9	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All
Application	Redhat	Single Sign-on	7.5.0	All	All	All

References

Reference	Source	L
KEYCLOAK-19177 Disable ECP flow by default for all Saml clients; ecp … · keycloak/keycloak@44000ca · GitHub	MISC	g
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	a
ECP SAML binding bypasses authentication flows · Advisory · keycloak/keycloak · GitHub	MISC	g
2007512 – (CVE-2021-3827) CVE-2021-3827 keycloak-server-spi-private: ECP SAML binding bypasses authentication flows	MISC	b
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

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**