



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 exploiting this flaw, an attacker can bypass the ECP binding flow and use any other authentication flow to authenticate. This flaw affects versions of Keycloak prior to 2022.0.0.

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	Link
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	e
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	t
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)