



CVE-2020-27846

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-27846
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-21 16:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	A signature verification vulnerability exists in crewjam/saml. This flaw allows an attacker to bypass SAML Authentication. Th

Risk And Classification

Problem Types: CWE-115

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Grafana	Grafana	All	All	All	All
Application	Grafana	Grafana	All	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	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Openshift Service Mesh	2.0	All	All	All
Application	Redhat	Openshift Service Mesh	2.0	All	All	All
Application	Saml Project	Saml	All	All	All	All
Application	Saml Project	Saml	All	All	All	All

References

Reference	Source	Link
-----------	--------	------

[SECURITY] Fedora 33 Update: grafana-7.3.6-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 32 Update: grafana-7.3.6-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
CVE-2020-27846 Grafana Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
1907670 – (CVE-2020-27846) CVE-2020-27846 crewjam/saml: authentication bypass in saml authentication	MISC	bugzilla.redhat.com
Grafana 6.7.5, 7.2.3, and 7.3.6 released with important security fix for Grafana Enterprise Grafana Labs	MISC	grafana.com
[SECURITY] Fedora 33 Update: grafana-7.3.6-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 32 Update: grafana-7.3.6-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Coordinated disclosure of XML round-trip vulnerabilities in Go library	MISC	mattermost.com
XML Processing · Advisory · crewjam/saml · GitHub	MISC	github.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.

Legacy QID Mappings

- [159224](#) Oracle Enterprise Linux Security Update for grafana (ELSA-2021-1859)
- [239449](#) Red Hat Update for grafana (RHSA-2021:1859)
- [940233](#) AlmaLinux Security Update for grafana (ALSA-2021:1859)
- [960816](#) Rocky Linux Security Update for grafana (RLSA-2021:1859)
- [982068](#) Go (go) Security Update for github.com/crewjam/saml (GHSA-4hq8-gmxx-h6w9)

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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