



# CVE-2020-13379

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-13379
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-03 19:15:00 UTC
<b>Updated</b>	2023-11-07 03:16:00 UTC
<b>Description</b>	The avatar feature in Grafana 3.0.1 through 7.0.1 has an SSRF Incorrect Access Control issue. This vulnerability allows an

## Risk And Classification

**Problem Types:** CWE-918

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Application	<a href="#">Grafana</a>	<a href="#">Grafana</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">E-series Performance Analyzer</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">E-series Performance Analyzer</a>	-	All	All	All
Application	<a href="#">Opensuse</a>	<a href="#">Backports Sle</a>	15.0	sp1	All	All
Application	<a href="#">Opensuse</a>	<a href="#">Backports Sle</a>	15.0	sp2	All	All
Application	<a href="#">Opensuse</a>	<a href="#">Backports Sle</a>	15.0	sp1	All	All
Application	<a href="#">Opensuse</a>	<a href="#">Backports Sle</a>	15.0	sp2	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All

## References

Reference	Source	Link	T
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>	M

oss-security - Re: Grafana 6.7.4 and 7.0.2 released with fix for CVE-2020-13379	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	M
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>	M
[SECURITY] Fedora 31 Update: grafana-6.7.4-1.fc31 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[security-announce] openSUSE-SU-2020:0892-1: moderate: Security update f	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	M
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>	M
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>	M
[security-announce] openSUSE-SU-2020:1105-1: moderate: Security update f	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	M
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>	M
Grafana 6.7.4 and 7.0.2 released with important security fix   Grafana Labs	CONFIRM	<a href="http://grafana.com">grafana.com</a>	V
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>	
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>	M
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>	
[security-announce] openSUSE-SU-2020:1611-1: moderate: Security update f	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	M
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>	
CVE-2020-13379 Grafana Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="http://security.netapp.com">security.netapp.com</a>	T
[security-announce] openSUSE-SU-2020:1646-1: moderate: Security update f	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	M
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>	
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>	M
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>	
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>	M
[SECURITY] Fedora 32 Update: grafana-6.7.4-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	T
Release Notes v7.0.x - Releases - Grafana Community	MISC	<a href="http://community.grafana.com">community.grafana.com</a>	R
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>	
Grafana 7.0.2 and 6.7.4 Security Update - Security Announcements - Grafana Community	MISC	<a href="http://community.grafana.com">community.grafana.com</a>	V
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>	M
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>	
CVE-2020-13379	MISC	<a href="http://rhyorater.github.io">rhyorater.github.io</a>	E
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>	M
[CVE-2020-13379] Unauthenticated DoS on Grafana 3.0.1 - 7.0.1   Mayank Malik	MISC	<a href="http://mostwanted002.cf">mostwanted002.cf</a>	E
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>	M
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>	
[SECURITY] Fedora 31 Update: grafana-6.7.4-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	T
[SECURITY] Fedora 31 Update: grafana-6.7.4-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	T

[SECURITY] Fedora 32 Update: grafana-6.7.4-1.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	M
Grafana 7.0.1 Denial Of Service ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	E
Release Notes v6.7.x - Releases - Grafana Community	MISC	<a href="https://community.grafana.com">community.grafana.com</a>	R
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
oss-security - Grafana 6.7.4 and 7.0.2 released with fix for CVE-2020-13379	CONFIRM	<a href="https://www.openwall.com">www.openwall.com</a>	M
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	c
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	c

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[376934](#) Alibaba Cloud Linux Security Update for grafana (ALINUX3-SA-2021:0073)

[501577](#) Alpine Linux Security Update for grafana

© [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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**