



# CVE-2019-13050

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

## Summary

<b>CVE</b>	CVE-2019-13050
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-06-29 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:03:00 UTC
<b>Description</b>	Interaction between the sks-keyserver code through 1.2.0 of the SKS keyserver network, and GnuPG through 2.2.16, make

## Risk And Classification

**Problem Types:** CWE-295

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">F5</a>	Traffix Signaling Delivery Controller	All	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Application	<a href="#">Gnupg</a>	<a href="#">Gnupg</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Application	<a href="#">Sks Keyserver Project</a>	<a href="#">Sks Keyserver</a>	All	All	All	All

## References

Reference
SKS Keyserver Network Under Attack · GitHub
[bookkeeper-issues] 20210628 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgr
Pony Mail!

Pony Mail!

[security-announce] openSUSE-SU-2019:1917-1: important: Security update

[SECURITY] Fedora 29 Update: gnupg2-2.2.17-1.fc29 - package-announce - Fedora Mailing-Lists

Marcus Brinkmann na Twitterze: "Recent reports on the #OpenPGP #keyserver certificate poisoning attacks have focused on the SKS keysern

myF5

support.f5.com/csp/article/K08654551

[SECURITY] Fedora 30 Update: gnupg2-2.2.17-1.fc30 - package-announce - Fedora Mailing-Lists

[Announce] GnuPG 2.2.17 released to mitigate attacks on key servers

[SECURITY] Fedora 30 Update: gnupg2-2.2.17-1.fc30 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 29 Update: gnupg2-2.2.17-1.fc29 - package-announce - Fedora Mailing-Lists

support.f5.com/csp/article/K08654551

Pony Mail!

[bookkeeper-issues] 20210629 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgr

[mina-dev] 20210225 [jira] [Created] (FTPSERVER-500) Security vulnerability in common/lib/log4j-1.2.17.jar

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

198808 Ubuntu Security Notification for GnuPG Vulnerability (USN-5431-1)

296078 Oracle Solaris 11.4 Support Repository Update (SRU) 16.4.0 Missing (CPUOCT2019)

770068 Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:0436)

940257 AlmaLinux Security Update for gnupg2 (ALSA-2020:4490)

960413 Rocky Linux Security Update for gnupg2 (RLSA-2020:4490)

© 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](#)**