



CVE-2018-14660

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

Summary

CVE	CVE-2018-14660
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-01 14:29:00 UTC
Updated	2023-02-13 04:51:00 UTC
Description	A flaw was found in glusterfs server through versions 4.1.4 and 3.1.2 which allowed repeated usage of GF_META_LOCK_...

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gluster	Glusterfs	All	All	All	All
Application	Gluster	Glusterfs	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Application	Redhat	Gluster Storage	3.0	All	All	All
Application	Redhat	Gluster Storage	3.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

References

Reference	Source
Red Hat Customer Portal	RECU

1635926 – (CVE-2018-14660) CVE-2018-14660 glusterfs: Repeat use of "GF_META_LOCK_KEY" xattr allows for memory exhaustion	MIS
Red Hat Customer Portal	RED
CVE-2018-14660 - Red Hat Customer Portal	MIS
GlusterFS: Multiple Vulnerabilities (GLSA 201904-06) — Gentoo security	GEN
[SECURITY] [DLA 2806-1] glusterfs security update	MLI
1635926 – (CVE-2018-14660) CVE-2018-14660 glusterfs: Repeat use of "GF_META_LOCK_KEY" xattr allows for memory exhaustion	COI
Red Hat Customer Portal	RED
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178862](#) Debian Security Update for glusterfs (DLA 2806-1)

[710178](#) Gentoo Linux GlusterFS Multiple Vulnerabilities Vulnerability (GLSA 201904-06)

© [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](#)