



# CVE-2018-10926

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

## Summary

<b>CVE</b>	CVE-2018-10926
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-09-04 15:29:00 UTC
<b>Updated</b>	2022-04-12 18:33:00 UTC
<b>Description</b>	A flaw was found in RPC request using gfs3_mknod_req supported by glusterfs server. An authenticated attacker could use

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Gluster</a>	<a href="#">Glusterfs</a>	All	All	All	All
Application	<a href="#">Gluster</a>	<a href="#">Glusterfs</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization Host</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization Host</a>	4.0	All	All	All

## References

Reference	Source	Link
[security-announce] openSUSE-SU-2020:0079-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
GlusterFS: Multiple Vulnerabilities (GLSA 201904-06) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
1613143 – (CVE-2018-10926) CVE-2018-10926 glusterfs: Device files can be created in arbitrary locations	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>
[SECURITY] [DLA 2806-1] glusterfs security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] [DLA 1510-1] glusterfs security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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](#)