



# CVE-2014-9637

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

## Summary

<b>CVE</b>	CVE-2014-9637
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-08-25 18:29:00 UTC
<b>Updated</b>	2017-08-30 01:16:00 UTC
<b>Description</b>	GNU patch 2.7.2 and earlier allows remote attackers to cause a denial of service (memory consumption and segmentation

## Risk And Classification

**Problem Types:** CWE-399

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.10	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	21	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	21	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Patch</a>	All	All	All	All
Operating System	<a href="#">Mageia</a>	<a href="#">Mageia</a>	4.0	All	All	All
Operating System	<a href="#">Mageia</a>	<a href="#">Mageia</a>	4.0	All	All	All

## References

Reference	Source	Link	Tags
USN-2651-1: GNU patch vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Patch, Tr

Mageia Advisory: MGASA-2015-0068 - Updated patch packages fix security vulnerabilities	CONFIRM	<a href="http://advisories.mageia.org">advisories.mageia.org</a>	Patch, Tr
[SECURITY] Fedora 20 Update: patch-2.7.5-1.fc20	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	Patch, Tr
[SECURITY] Fedora 21 Update: patch-2.7.3-1.fc21	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	Patch, Tr
GNU patch 'set_hunkmax()' Function Denial of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Par
Bug 1185262 – CVE-2014-9637 patch: local denial of service with a crafted patch	CONFIRM	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Tra
oss-security - Re: CVE request: directory traversal flaw in patch	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing Li
patch.git - GNU patch	CONFIRM	<a href="http://git.savannah.gnu.org">git.savannah.gnu.org</a>	Issue Tra
GNU patch - Bugs: bug #44051, fuzzed diff can make patch to eat... [Savannah]	CONFIRM	<a href="http://savannah.gnu.org">savannah.gnu.org</a>	Issue Tra
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

671067 EulerOS Security Update for patch (EulerOS-SA-2019-2645)

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

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