



# CVE-2019-13638

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

## Summary

<b>CVE</b>	CVE-2019-13638
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-07-26 13:15:00 UTC
<b>Updated</b>	2023-11-07 03:03:00 UTC
<b>Description</b>	GNU patch through 2.7.6 is vulnerable to OS shell command injection that can be exploited by opening a crafted patch file t

## Risk And Classification

### Problem Types: CWE-78

## 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>	10.0	All	All	All
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>	10.0	All	All	All
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
Application	<a href="#">Gnu</a>	<a href="#">Patch</a>	2.7.6	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Patch</a>	2.7.6	All	All	All

## References

Reference
<a href="#">CVE-2019-13638</a>
<a href="#">Red Hat Customer Portal</a>
<a href="#">Red Hat Customer Portal</a>
<a href="#">[SECURITY] Fedora 30 Update: patch-2.7.6-11.fc30 - package-announce - Fedora Mailing-Lists</a>
<a href="#">August 2019 GNU patch Vulnerabilities in NetApp Products   NetApp Product Security</a>
<a href="#">Debian -- Security Information -- DSA-4489-1 patch</a>

Bugtraq: Details about recent GNU patch vulnerabilities

Bugtraq: [SECURITY] [DSA 4489-1] patch security update

GitHub - irsl/gnu-patch-vulnerabilities: The GNU patch utility was prone vulnerable to multiple attacks through version 2.7.6. You can find my r

Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

patch.git - GNU patch

[SECURITY] Fedora 30 Update: patch-2.7.6-11.fc30 - package-announce - Fedora Mailing-Lists

Patch: Multiple vulnerabilities (GLSA 201908-22) — Gentoo security

GNU patch Command Injection / Directory Traversal ≈ Packet Storm

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[296079](#) Oracle Solaris 11.4 Support Repository Update (SRU) 15.5.0 Missing (CPUOCT2019)

[377009](#) Alibaba Cloud Linux Security Update for patch (ALINUX2-SA-2019:0114)

[378297](#) Virtuozzo Linux Security Update for patch (VZLSA-2019:2964)

[500513](#) Alpine Linux Security Update for patch

[504272](#) Alpine Linux Security Update for patch

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

[900088](#) CBL-Mariner Linux Security Update for patch 2.7.6

[901475](#) Common Base Linux Mariner (CBL-Mariner) Security Update for patch (6790-1)

[903211](#) Common Base Linux Mariner (CBL-Mariner) Security Update for patch (2563)

[906212](#) Common Base Linux Mariner (CBL-Mariner) Security Update for patch (2563-1)

[906275](#) Common Base Linux Mariner (CBL-Mariner) Security Update for patch (6790-2)

© [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)**