



CVE-2014-4877

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

Summary

CVE	CVE-2014-4877
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-29 10:55:00 UTC
Updated	2017-02-17 02:59:00 UTC
Description	Absolute path traversal vulnerability in GNU Wget before 1.16, when recursion is enabled, allows remote FTP servers to wr

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Wget	1.12	All	All	All
Application	Gnu	Wget	1.13	All	All	All
Application	Gnu	Wget	1.13.1	All	All	All
Application	Gnu	Wget	1.13.2	All	All	All
Application	Gnu	Wget	1.13.3	All	All	All
Application	Gnu	Wget	1.13.4	All	All	All
Application	Gnu	Wget	1.14	All	All	All
Application	Gnu	Wget	1.12	All	All	All
Application	Gnu	Wget	1.13	All	All	All
Application	Gnu	Wget	1.13.1	All	All	All
Application	Gnu	Wget	1.13.2	All	All	All
Application	Gnu	Wget	1.13.3	All	All	All
Application	Gnu	Wget	1.13.4	All	All	All
Application	Gnu	Wget	1.14	All	All	All
Application	Gnu	Wget	All	All	All	All

References

Reference	Source	Link
Oracle Bulletin Board Update - January 2015	CONFIRM	www.oracle.com
Gentoo Linux Documentation -- GNU Wget: Arbitrary code execution	GENTOO	security.gentoo.org
[security-announce] SUSE-SU-2014:1408-1: important: Security update for	SUSE	lists.opensuse.org
Debian -- Security Information -- DSA-3062-1 wget	DEBIAN	www.debian.org
Document Display HPE Support Center	CONFIRM	h20566.www2.hp.com
McAfee KnowledgeBase - McAfee Security Bulletin - Data Loss Prevention hotfix resolves two security issues	CONFIRM	kc.mcafee.com
Vulnerability Note VU#685996 - GNU Wget creates arbitrary symbolic links during recursive FTP download	CERT-VN	www.kb.cert.org
Mageia Advisory: MGASA-2014-0431 - Updated wget packages fix CVE-2014-4877	CONFIRM	advisories.mageia.org
USN-2393-1: Wget vulnerability Ubuntu	UBUNTU	www.ubuntu.com
Add module for CVE-2014-4877 (Wget) by hmoore-r7 · Pull Request #4088 · rapid7/metasploit-framework · GitHub	MISC	github.com
Metasploit: R7-2014-15: GNU Wget FTP Symlink Arbitrary Filesystem Access SecurityStreet	MISC	community.securitystreet.com
wget.git - GNU Wget	CONFIRM	git.savannah.gnu.org
Red Hat Customer Portal	REDHAT	rhn.redhat.com
wget.git - GNU Wget	CONFIRM	git.savannah.gnu.org
openSUSE-SU-2014:1380-1: moderate: update for wget	SUSE	lists.opensuse.org
Bug 1139181 – CVE-2014-4877 wget: FTP symlink arbitrary filesystem access	CONFIRM	bugzilla.redhat.com
GNU Wget CVE-2014-4877 Symlink Vulnerability	BID	www.securityfocus.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
[Bug-wget] GNU wget 1.16 released	MLIST	lists.gnu.org
[security-announce] SUSE-SU-2014:1366-1: important: Security update for	SUSE	lists.opensuse.org
Document Display HPE Support Center	CONFIRM	h20566.www2.hp.com
Support / Security / Advisories // MDVSA-2015:121 Mandriva	MANDRIVA	www.mandriva.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report