



CVE-2014-2972

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

Summary

CVE	CVE-2014-2972
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-04 17:55:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	expand.c in Exim before 4.83 expands mathematical comparisons twice, which allows local users to gain privileges and execute arbitrary code.

Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:P/A:P

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Exim	Exim	4.00	All	All	All

Application	Exim	Exim	4.01	All	All	All
Application	Exim	Exim	4.02	All	All	All
Application	Exim	Exim	4.03	All	All	All
Application	Exim	Exim	4.04	All	All	All
Application	Exim	Exim	4.05	All	All	All
Application	Exim	Exim	4.10	All	All	All
Application	Exim	Exim	4.11	All	All	All
Application	Exim	Exim	4.12	All	All	All
Application	Exim	Exim	4.14	All	All	All
Application	Exim	Exim	4.20	All	All	All
Application	Exim	Exim	4.21	All	All	All
Application	Exim	Exim	4.22	All	All	All
Application	Exim	Exim	4.23	All	All	All
Application	Exim	Exim	4.24	All	All	All
Application	Exim	Exim	4.30	All	All	All
Application	Exim	Exim	4.31	All	All	All
Application	Exim	Exim	4.32	All	All	All
Application	Exim	Exim	4.33	All	All	All
Application	Exim	Exim	4.34	All	All	All
Application	Exim	Exim	4.40	All	All	All
Application	Exim	Exim	4.41	All	All	All
Application	Exim	Exim	4.42	All	All	All
Application	Exim	Exim	4.43	All	All	All
Application	Exim	Exim	4.44	All	All	All
Application	Exim	Exim	4.50	All	All	All
Application	Exim	Exim	4.51	All	All	All
Application	Exim	Exim	4.52	All	All	All
Application	Exim	Exim	4.53	All	All	All
Application	Exim	Exim	4.54	All	All	All
Application	Exim	Exim	4.60	All	All	All
Application	Exim	Exim	4.61	All	All	All
Application	Exim	Exim	4.62	All	All	All
Application	Exim	Exim	4.63	All	All	All
Application	Exim	Exim	4.64	All	All	All
Application	Exim	Exim	4.65	All	All	All
Application	Exim	Exim	4.66	All	All	All

Application	Exim	Exim	4.67	All	All	All
Application	Exim	Exim	4.68	All	All	All
Application	Exim	Exim	4.69	All	All	All
Application	Exim	Exim	4.70	All	All	All
Application	Exim	Exim	4.71	All	All	All
Application	Exim	Exim	4.72	All	All	All
Application	Exim	Exim	4.73	All	All	All
Application	Exim	Exim	4.74	All	All	All
Application	Exim	Exim	4.75	All	All	All
Application	Exim	Exim	4.76	All	All	All
Application	Exim	Exim	4.77	All	All	All
Application	Exim	Exim	4.80	All	All	All
Application	Exim	Exim	4.80.1	All	All	All
Application	Exim	Exim	4.82	All	All	All
Application	Exim	Exim	All	All	All	All

Vendor Declared Affected Products					
Source	Vendor	Product	Version	Platforms	
CNA	Na	N/a	affected n/a	Not specified	

References		
Reference	Source	Link
Bug 1122552 – CVE-2014-2972 exim: local code execution via string expansion	af854a3a-2127-422b-91ae-364da2661108	bugzilla.redhat.com
git.exim.org Git - exim.git/commitdiff	af854a3a-2127-422b-91ae-364da2661108	git.exim.org
[exim] Exim 4.83 Released	af854a3a-2127-422b-91ae-364da2661108	lists.exim.org
[exim] Exim Security Advisory CVE-2014-2972	af854a3a-2127-422b-91ae-364da2661108	lists.exim.org
[SECURITY] Fedora 19 Update: exim-4.80.1-4.fc19	af854a3a-2127-422b-91ae-364da2661108	lists.fedoraproject.org
Exim: Arbitrary code execution (GLSA 201607-12) — Gentoo security	af854a3a-2127-422b-91ae-364da2661108	security.gentoo.org
[SECURITY] Fedora 20 Update: exim-4.80.1-7.fc20	af854a3a-2127-422b-91ae-364da2661108	lists.fedoraproject.org
USN-2933-1: Exim vulnerabilities Ubuntu	af854a3a-2127-422b-91ae-364da2661108	www.ubuntu.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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)