



CVE-2010-4345

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2010-4345
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-12-14 16:00:04 UTC
Updated	2026-04-21 20:30:40 UTC
Description	Exim 4.72 and earlier allows local users to gain privileges by leveraging the ability of the exim user account to specify an alt

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.068560000 probability, percentile 0.914040000 (date 2026-04-23)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Unknown

Problem Types: NVD-CWE-noinfo | CWE-77 | n/a | CWE-77 CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.9		AV:L/AC:MAu:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

CISA Known Exploited Vulnerability

Vendor	Exim
Product	Exim
Name	Exim Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2010-4345

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All

Operating System	Debian	Debian Linux	5.0	All	All	All
Application	Exim	Exim	All	All	All	All
Operating System	Opensuse	Opensuse	11.1	All	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Metasploit Penetration Testing Framework - Module Browser	af854a3a-2127-422b-91ae-36
Debian -- Security Information -- DSA-2154-1 exim4	af854a3a-2127-422b-91ae-36
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a4
Re: [exim-dev] [Exim-maintainers] Remote root vulnerability in Exim	af854a3a-2127-422b-91ae-36
oss-security - 21Nails: Multiple vulnerabilities in Exim	af854a3a-2127-422b-91ae-36
USN-1060-1: Exim vulnerabilities Ubuntu	af854a3a-2127-422b-91ae-36
Exim code-execution bug, now with root access • The Register	af854a3a-2127-422b-91ae-36
US-CERT Vulnerability Note VU#758489	af854a3a-2127-422b-91ae-36
Critical: Exim security update (CVE-2010-4345) - cPanel Inc.	af854a3a-2127-422b-91ae-36
Support	af854a3a-2127-422b-91ae-36
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-36
Re: [exim-dev] Remote root vulnerability in Exim	af854a3a-2127-422b-91ae-36
[security-announce] SUSE Security Announcement: exim (SUSE-SA:2010:059)	af854a3a-2127-422b-91ae-36
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-36
[exim-dev] Remote root vulnerability in Exim	af854a3a-2127-422b-91ae-36
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-36
Debian update for exim4 - Secunia.com	af854a3a-2127-422b-91ae-36
Exim ALT_CONFIG_ROOT_ONLY 'exim' User Local Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-36
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-36
Webmail - OVH	af854a3a-2127-422b-91ae-36
Debian -- Security Information -- DSA-2131-1 exim4	af854a3a-2127-422b-91ae-36
SUSE update for exim - Advisories - Community	af854a3a-2127-422b-91ae-36
Red Hat update for exim - Advisories - Community	af854a3a-2127-422b-91ae-36
SecurityFocus	af854a3a-2127-422b-91ae-36

Bug 662012 – CVE-2010-4345 exim privilege escalation	af854a3a-2127-422b-91ae-36
oss-security - Exim remote root	af854a3a-2127-422b-91ae-36
SecurityTracker.com Archives - Exim Configuration File Capability Lets Local Users Gain Elevated Privileges	af854a3a-2127-422b-91ae-36
Security Advisory SA43243 - Ubuntu update for exim4 - Secunia	af854a3a-2127-422b-91ae-36
Bug 1044 – CVE-2010-4345 exim privilege escalation	af854a3a-2127-422b-91ae-36
Red Hat Customer Portal	MITRE
access.redhat.com CVE-2010-4345	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-25T00:00:00.000Z	CVE-2010-4345 added to CISA KEV

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](#)