CVE-2010-4344

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2010-4344
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 20:31:04 UTC
Description	Heap-based buffer overflow in the string_vformat function in string.c in Exim before 4.70 allows remote attackers to execute

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.530640000 probability, percentile 0.979710000 (date 2026-04-23)

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

Problem Types: CWE-787 | n/a | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9.3		AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

CISA Known Exploited Vulnerability

Vendor	Exim
Product	Exim
Name	Exim Heap-Based Buffer Overflow Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2010-4344

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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-91
Atmail Blog	af854a3a-2127-422b-91
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91
oss-security - 21Nails: Multiple vulnerabilities in Exim	af854a3a-2127-422b-91
Bug 787 – memory corruption in string_format code	af854a3a-2127-422b-91
Ubuntu update for exim4 - Advisories - Community	af854a3a-2127-422b-91
access.redhat.com	af854a3a-2127-422b-91
Exim code-execution bug, now with root access • The Register	af854a3a-2127-422b-91
Red Hat update for exim - Advisories - Community	af854a3a-2127-422b-91
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91
Re: [exim-dev] Remote root vulnerability in Exim	af854a3a-2127-422b-91
[security-announce] SUSE Security Announcement: exim (SUSE-SA:2010:059)	af854a3a-2127-422b-91
SecurityTracker.com Archives - Exim Buffer Overfow in string_format() Lets Remote Users Execute Arbitrary Code	af854a3a-2127-422b-91
Exim Crafted Header Remote Code Execution Vulnerability	af854a3a-2127-422b-91
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91
[exim-dev] Remote root vulnerability in Exim	af854a3a-2127-422b-91
www.osvdb.org/69685	af854a3a-2127-422b-91
Exim Weaknesses and Buffer Overflow Vulnerability - Advisories - Community	af854a3a-2127-422b-91
Debian -- Security Information -- DSA-2131-1 exim4	af854a3a-2127-422b-91
Debian update for exim4 - Advisories - Community	af854a3a-2127-422b-91
SUSE update for exim - Advisories - Community	af854a3a-2127-422b-91
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b
Bug 661756 – CVE-2010-4344 exim remote code execution flaw	af854a3a-2127-422b-91
SecurityFocus	af854a3a-2127-422b-91

ftp.exim.org/pub/exim/ChangeLogs/ChangeLog-4.70	af854a3a-2127-422b-91
US-CERT Vulnerability Note VU#682457	af854a3a-2127-422b-91
oss-security - Exim remote root	af854a3a-2127-422b-91
git.exim.org Git - exim.git/commit	af854a3a-2127-422b-91
USN-1032-1: Exim vulnerability | Ubuntu	af854a3a-2127-422b-91
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91
Exim Remote Memory Corruption Vulnerability Notification (CVE-2010-4344) - cPanel Inc.	af854a3a-2127-422b-91
Red Hat Customer Portal	MITRE
access.redhat.com | CVE-2010-4344	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-2010-4344 added to CISA KEV

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