CVE-2016-5384

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

Summary

CVE	CVE-2016-5384
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-08-13 01:59:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	fontconfig before 2.12.1 does not validate offsets, which allows local users to trigger arbitrary free calls and consequently cc

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: 0.001950000 probability, percentile 0.411470000 (date 2026-05-09)

Problem Types: CWE-415 | n/a

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
2.0	nvd@nist.gov	Primary	4.6		AV:L/AC:L/Au:N/C:P/I:P/A:P

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

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
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Application	Fontconfig Project	Fontconfig	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
Red Hat Customer Portal	af854a3a-2127-42
Fontconfig CVE-2016-5384 Local Privilege Escalation Vulnerability	af854a3a-2127-42
fontconfig - Font customization and configuration library (mirrored from https://gitlab.freedesktop.org/fontconfig/fontconfig)	af854a3a-2127-42

[SECURITY] Fedora 24 Update: fontconfig-2.11.94-7.fc24 - package-announce - Fedora Mailing-Lists	af854a3a-2127-42
[SECURITY] Fedora 23 Update: fontconfig-2.11.94-5.fc23 - package-announce - Fedora Mailing-Lists	af854a3a-2127-42
Debian -- Security Information -- DSA-3644-1 fontconfig	af854a3a-2127-42
[Fontconfig] fontconfig: Branch 'master' - 3 commits	af854a3a-2127-42
USN-3063-1: Fontconfig vulnerability | Ubuntu	af854a3a-2127-42
[SECURITY] Fedora 23 Update: fontconfig-2.11.94-5.fc23 - package-announce - Fedora Mailing-Lists	MITRE
[SECURITY] Fedora 24 Update: fontconfig-2.11.94-7.fc24 - package-announce - Fedora Mailing-Lists	MITRE
Red Hat Customer Portal	MITRE
CVE-2016-5384 - Red Hat Customer Portal	MITRE
1350891 – (CVE-2016-5384) CVE-2016-5384 fontconfig: Possible double free due to insufficiently validated cache files	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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