CVE-2010-4577

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

Summary

CVE	CVE-2010-4577
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-12-22 01:00:03 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The CSSParser::parseFontFaceSrc function in WebCore/css/CSSParser.cpp in WebKit, as used in Google Chrome before

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

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

Problem Types: CWE-125 | CWE-843 | n/a | CWE-125 CWE-125 Out-of-bounds Read | CWE-843 CWE-843 Access of Resource Using Incompatible Type ('Type Confusion')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

None

ntegrity

None

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

ntegrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Fedoraproject	Fedora	13	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Google	Chrome Os	All	All	All	All
Application	Webkitgtk	Webkitgtk	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
[SECURITY] Fedora 13 Update: webkitgtk-1.2.6-1.fc13	af854a3a-2127-422b-91ae-364d
Repository / Oval Repository	af854a3a-2127-422b-91ae-364d

Changeset 72685 for trunk/WebCore/css/CSSParser.cpp – WebKit	af854a3a-2127-422b-91ae-364d
667025 – (CVE-2010-4577) CVE-2010-4577 webkit: CSS Font Face Parsing Type Confusion Vulnerability	af854a3a-2127-422b-91ae-364d
WebKit CSS Token Sequences Handling Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364d
Changeset 72685 – WebKit	af854a3a-2127-422b-91ae-364d
Access Denied	af854a3a-2127-422b-91ae-364d
Google Chrome Releases: Stable, Beta Channel Updates	af854a3a-2127-422b-91ae-364d
63866 - chromium - An open-source project to help move the web forward. - Monorail	af854a3a-2127-422b-91ae-364d
Webmail - OVH	af854a3a-2127-422b-91ae-364d
Support	af854a3a-2127-422b-91ae-364d
Debian -- Security Information -- DSA-2188-1 webkit	af854a3a-2127-422b-91ae-364d
Gentoo Linux Documentation -- Chromium: Multiple vulnerabilities	af854a3a-2127-422b-91ae-364d
Red Hat update for webkitgtk - Secunia.com	af854a3a-2127-422b-91ae-364d
Gentoo update for chromium - Secunia.com	af854a3a-2127-422b-91ae-364d
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.