CVE-2011-3078

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

Summary

CVE	CVE-2011-3078
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-05-01 10:12:04 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Use-after-free vulnerability in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-416 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All

Application	Apple	Itunes	All	All	All	All
Application	Apple	Safari	All	All	All	All
Application	Google	Chrome	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
Google Chrome Prior to 18.0.1025.168 Multiple Security Vulnerabilities
IBM X-Force Exchange
About the security content of Safari 6
osvdb.org/81643
Chrome Releases: Stable Channel Update
About the security content of iTunes 10.7
Issue 106413 - chromium - Heap-use-after-free in WebCore::RenderBlock::checkFloatsInCleanLine - An open-source project to help move the
APPLE-SA-2012-07-25-1 Safari 6.0
Gentoo Linux Documentation -- Chromium: Multiple vulnerabilities
Google Chrome Multiple Flaws Let Remote Users Execute Arbitrary Code - SecurityTracker
APPLE-SA-2012-09-12-1 iTunes 10.7
About the security content of iOS 6
APPLE-SA-2012-09-19-1 iOS 6
Security Alerts - Secunia
Repository / Oval Repository
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**