CVE-2011-3050

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

Summary

CVE	CVE-2011-3050
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-03-22 16:55:00 UTC
Updated	2020-04-14 16:06:00 UTC
Description	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 17.0.963.83 allo

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Application	Apple	Itunes	All	All	All	All
Application	Apple	Itunes	All	All	All	All
Application	Apple	Safari	All	All	All	All
Application	Apple	Safari	All	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All

References

Reference
Issue 113902 - chromium - Heap-use-after-free in WebCore::InlineBox::root - An open-source project to help move the web forward. - Google
Chrome Releases: Stable Channel Update
APPLE-SA-2012-07-25-1 Safari 6.0
APPLE-SA-2012-09-12-1 iTunes 10.7

Security Alerts - Secunia
Google Chrome Prior to 17.0.963.83 Multiple Security Vulnerabilities
IBM X-Force Exchange
APPLE-SA-2012-09-19-1 iOS 6
[security-announce] openSUSE-SU-2012:0466-1: important: update for chrom
About the security content of iTunes 10.7
80288
About the security content of Safari 6
About Secunia Research | Flexera
Google Chrome Multiple Flaws Let Remote Users Execute Arbitrary Code - SecurityTracker
Gentoo Linux Documentation -- Chromium: Multiple vulnerabilities
Repository / Oval Repository
About the security content of iOS 6
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**