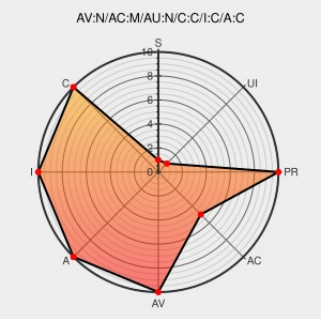
CVE-2010-1823

Published on: 09/24/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:05 PM UTC

CVE-2010-1823

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Itunes from Apple contain the following vulnerability:

Use-after-free vulnerability in WebKit before r65958, as used in Google Chrome before 6.0.472.59, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger use of document APIs such as document.close during parsing, as demonstrated by a Cascading Style Sheets (CSS) file referencing an invalid SVG font, aka rdar problem 8442098.

CVE-2010-1823 has been assigned by product-security@apple.com to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Google Chrome Releases: Stable, Beta Channel Updates	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2010/09/stable-beta-channel-updates_14.html
About the security content of Safari 5.1 and Safari 5.0.6	Third Party Advisory support.apple.com text/html	CONFIRM support.apple.com/kb/HT4808
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2011-0212
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org	OVAL oval:org.mitre.oval:def:7405

	text/html	
Access Denied	Permissions Required bugs.webkit.org text/html	CONFIRM bugs.webkit.org/show_bug.cgi?id=43055
APPLE-SA-2011-07-20-1 Safari 5.1 and Safari 5.0.6	Mailing List Third Party Advisory lists.apple.com text/html	APPLE APPLE-SA-2011-07-20-1
50250 - chromium - An open-source project to help move the web forward. - Monorail	Issue Tracking Patch Vendor Advisory code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=50250
Bug 44533 – XMLDocumentParser needs to implement DocumentParser::detach()	Issue Tracking Patch Third Party Advisory bugs.webkit.org text/html	CONFIRM bugs.webkit.org/show_bug.cgi?id=44533
APPLE-SA-2011-10-11-1 iTunes 10.5	Mailing List Third Party Advisory lists.apple.com text/html	APPLE APPLE-SA-2011-10-11-1
About the security content of iTunes 10.5	Third Party Advisory support.apple.com text/html	CONFIRM support.apple.com/kb/HT4981
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:002	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SR:2011:002
SUSE update for Multiple Packages - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 43068

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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

cpe:2.3:a:apple:itunes:*:*:*:*:*:*:*:*:

cpe:2.3:a:apple:itunes:*:*:*:*:*:*:*:*:

cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*:

cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→