

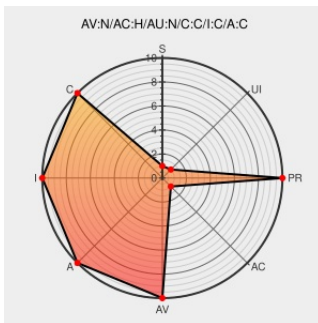


CVE-2007-2175

Published on: 04/24/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:43 PM UTC

CVE-2007-2175

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Safari](#) from [Apple](#) contain the following vulnerability:

Apple QuickTime Java extensions (QTJava.dll), as used in Safari and other browsers, and when Java is enabled, allows remote attackers to execute arbitrary code via parameters to the toQTPointer method in quicktime.util.QTHandleRef, which can be used to modify arbitrary memory when creating QTPointerRef objects, as demonstrated during the "PWN 2 OWN" contest at CanSecWest 2007.

CVE-2007-2175 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.6 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

HIGH

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

No Description Provided

[www.osvdb.org](#)

[OSVDB 34178](#)

Inactive Link Not Archived

Matasano Chargen » Hot Off The Matasano SMS Queue: CanSec Macbook Challenge Won

[web.archive.org](#)

[text/html](#)

Inactive Link Not Archived

[MISC www.matasano.com/log/806/hot-off-the-matasano-sms-queue-cansec-macbook-challenge-won/](#)

CanSecWest Applied Security Conference: Vancouver, British Columbia, Canada

[cansecwest.com](#)

[text/html](#)

[MISC cansecwest.com/post/2007-04-20-14:54:00.First_Mac_Hacked_Cancel_Or_Allow](#)

About the security content of QuickTime 7.1.6

[web.archive.org](#)

[text/html](#)

Inactive Link Not Archived

[CONFIRM docs.info.apple.com/article.html?artnum=305446](#)

APPLE-SA-2007-05-01 QuickTime 7.1.6	lists.apple.com text/html	 APPLE APPLE-SA-2007-05-01
No Description Provided	www.matasano.com Inactive Link Not Archived	 MISC www.matasano.com/log/812/breaking-macbook-vuln-in-quicktime-affects-win32-apple-code/
SecurityTracker.com Archives - Apple QuickTime Java Bug Lets Remote Users Execute Arbitrary Code	www.securitytracker.com text/html	 SECTRAK 1017950
VU#420668 - Apple QuickTime for Java QTPointerRef heap memory corruption vulnerability	US Government Resource www.kb.cert.org text/html	 CERT-VN VU#420668
SecurityFocus	web.archive.org text/html Inactive Link Not Archived	 BUGTRAQ 20070501 ZDI-07-023: Apple QTJava toQTPointer() Pointer Arithmetic Memory Overwrite Vulnerability
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF quicktime-unspecified-code-execution(33827)
Safari zero-day exploit nets \$10,000 prize The Register	www.theregister.co.uk text/xml	 MISC www.theregister.co.uk/2007/04/20/pwn-2-own_winner/
ZDI-07-023	www.zerodayinitiative.com text/html	 MISC www.zerodayinitiative.com/advisories/ZDI-07-023.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Safari	All	All	All	All
Application	Apple	Safari	All	All	All	All
cpe:2.3:a:apple:safari:*****:.*.*						
cpe:2.3:a:apple:safari:*****:.*.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

[site](#). This site includes MITRE data granted under the following [license](#).

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