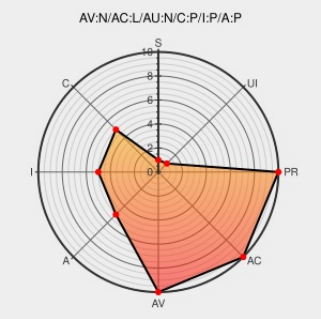
CVE-2005-3711

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-3711

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



Certain versions of Quicktime from Apple contain the following vulnerability:

Integer overflow in Apple Quicktime before 7.0.4 allows remote attackers to execute arbitrary code via a TIFF image file with modified (1) "strips" (StripByteCounts) or (2) "bands" (StripOffsets) values.

CVE-2005-3711 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
RETIRED: Apple QuickTime Multiple Code Execution Vulnerabilities	Patch, cve.report (archive), text/html	BID 16202
SecurityTracker.com Archives - Apple QuickTime TIFF Integer Overflow May Let Remote Users Execute Arbitrary Code	securitytracker.com, text/html	SECTRACK 1015465
SecurityFocus	www.securityfocus.com, text/html	BUGTRAQ 20060112 Fortinet Advisory - Apple QuickTime Player StripOffsets Improper Memory Access
Neohapsis Archives - Full Disclosure List - #0442 - [Full-disclosure] Fortinet Advisory - Apple QuickTime Player StripByteCounts Buffer Overflow Vulnerability	web.archive.org, text/html, Inactive Link, Not Archived	FULLDISC 20060112 Fortinet Advisory - Apple QuickTime Player StripByteCounts Buffer Overflow Vulnerability

SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060112 Fortinet Advisory - Apple QuickTime Player StripByteCounts Buffer Overflow Vulnerability
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 22337
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-0128
About the security content of QuickTime 7.0.4	Patch web.archive.org text/html Inactive Link Not Archived	APPLE APPLE-SA-2006-01-10
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF quicktime-tiff-overflow(24059)
Secunia - Advisories - QuickTime Multiple Image/Media File Handling Vulnerabilities	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18370

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Quicktime	7.0	All	All	All
Application	Apple	Quicktime	7.0.1	All	All	All
Application	Apple	Quicktime	7.0.2	All	All	All
Application	Apple	Quicktime	7.0	All	All	All
Application	Apple	Quicktime	7.0.1	All	All	All
Application	Apple	Quicktime	7.0.2	All	All	All
Application	Apple	Quicktime	All	All	All	All

cpe:2.3:a:apple:quicktime:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:apple:quicktime:7.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:apple:quicktime:7.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:apple:quicktime:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:apple:quicktime:7.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:apple:quicktime:7.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:apple:quicktime:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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