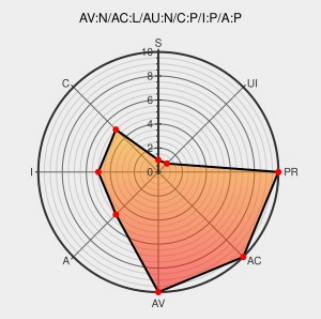
CVE-2005-2340

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

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2340

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



Certain versions of Quicktime from Apple contain the following vulnerability:

Heap-based buffer overflow in Apple Quicktime before 7.0.4 allows remote attackers to execute arbitrary code via a crafted (1) QuickTime Image File (QTIF), (2) PICT, or (3) JPEG format image with a long data field.

CVE-2005-2340 has been assigned by cert@cert.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
eCrimeLabs - Helps you mitigate your cyber threats	Vendor Advisory, www.cirt.dk, application/pdf, Inactive Link, Not Archived	MISC www.cirt.dk/advisories/cirt-41-advisory.pdf
SecurityFocus	www.securityfocus.com, text/html	BUGTRAQ 20060111 [EEYEB-20051220] Apple QuickTime QTIF Stack Overflow
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF quicktime-qtif-bo(24054)
Apple QuickTime PictureViewer JPEG/PICT File Buffer Overflow	Exploit	BID 16212

Vulnerability	cve.report (archive) text/html	
SecurityTracker.com Archives - Apple QuickTime QTIF Buffer Overflow May Let Remote Users Execute Arbitrary Code	Patch securitytracker.com text/html	SECTRACK 1015463
No Description Provided	Patch www.osvdb.org Inactive Link Not Archived	OSVDB 22335
US-CERT Technical Cyber Security Alert TA06-011A -- Apple QuickTime Vulnerabilities	Patch Third Party Advisory US Government Resource www.us-cert.gov text/html	CERT TA06-011A
Neohapsis Archives - Full Disclosure List - #0392 - [Full-disclosure] [CIRT.DK] Apple QuickTime 7.0.3 and earlier - JPG/PICT Buffer Overflow	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20060111 [CIRT.DK] Apple QuickTime 7.0.3 and earlier - JPG/PICT Buffer Overflow
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060111 Updated Advisories - Incorrect CVE Information
Neohapsis Archives - Full Disclosure List - #0402 - [Full-disclosure] Updated Advisories - Incorrect CVE Information	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20060111 Updated Advisories - Incorrect CVE Information
No Description Provided	Patch www.osvdb.org Inactive Link Not Archived	OSVDB 22334
No Description Provided	Patch www.osvdb.org Inactive Link Not Archived	OSVDB 22333
Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-0128
Neohapsis Archives - Full Disclosure List - #0398 - [Full-disclosure] [EEYEB-20051220] Apple QuickTime QTIF Stack Overflow	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	FULLDISC 20060111 [EEYEB-20051220] Apple QuickTime QTIF Stack Overflow
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
US-CERT Vulnerability Note VU#629845	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#629845
CXSecurity - IDS	securityreason.com text/html	SREASON 332
Secunia - Advisories - QuickTime Multiple Image/Media File Handling Vulnerabilities	Patch Vendor Advisory web.archive.org	SECUNIA 18370

	text/html	
US-CERT Vulnerability Note VU#687201	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#687201

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