



CVE-2008-1017

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

Summary

CVE	CVE-2008-1017
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-04-04 17:44:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Heap-based buffer overflow in clipping region (aka crgn) atom handling in quicktime.qts in Apple QuickTime before 7.4.5 all

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:P

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Quicktime	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				Source
IBM X-Force Exchange				af854a3a-21
APPLE-SA-2008-07-10 Apple TV 2.1				af854a3a-21
Apple QuickTime Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-21
Apple QuickTime Multiple Remote Vulnerabilities				af854a3a-21
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				af854a3a-21
About the security content of QuickTime 7.4.5				af854a3a-21
Apple TV Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-21
SecurityTracker.com Archives - QuickTime Heap Overflow in Parsing 'crgn' Atoms Lets Remote Users Execute Arbitrary Code				af854a3a-21
US-CERT Technical Cyber Security Alert TA08-094A -- Apple Updates for Multiple Vulnerabilities				af854a3a-21
Webmail - OVH				af854a3a-21
Zero Day Initiative				af854a3a-21
SecurityFocus				af854a3a-21
CVE Program record				CVE.ORG
NVD vulnerability detail				NVD
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				