CVE-2008-1581

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

Summary

CVE	CVE-2008-1581
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-06-10 18:32:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Heap-based buffer overflow in Apple QuickTime before 7.5 on Windows allows remote attackers to cause a denial of servic

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

Operating System	Microsoft	Windows Vista	All	All	All	All
Operating System	Microsoft	Windows Xp	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
US-CERT Technical Cyber Security Alert TA08-162C -- Apple Quicktime Updates for Multiple Vulnerabilities	af854a3a-2127-422b-9
About Secunia Research | Flexera	af854a3a-2127-422b-9
About the security content of QuickTime 7.5	af854a3a-2127-422b-9
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-9
Apple QuickTime 'PICT' Image 'PixData' Structures Handling Heap Overflow Vulnerability	af854a3a-2127-422b-9
RETIRED: Apple QuickTime Multiple Arbitrary Code Execution Vulnerabilities	af854a3a-2127-422b-9
APPLE-SA-2008-06-09 QuickTime 7.5	af854a3a-2127-422b-9
QuickTime PICT File PixData Structure Heap Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-9
SecurityFocus	af854a3a-2127-422b-9
IBM X-Force Exchange	af854a3a-2127-422b-9
Vulnerabilities - Secunia Research - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-9
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.