



CVE-2002-0252

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2002-0252
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-05-29 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in Apple QuickTime Player 5.01 and 5.02 allows remote web servers to execute arbitrary code via a response that is larger than the buffer. The vulnerability exists in the QuickTime Player 5.01 and 5.02. The vulnerability is caused by a buffer overflow in the QuickTime Player 5.01 and 5.02. The vulnerability is caused by a buffer overflow in the QuickTime Player 5.01 and 5.02. The vulnerability is caused by a buffer overflow in the QuickTime Player 5.01 and 5.02.

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/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	5.0.1	All	All	All

Application	Apple	Quicktime	5.0.2	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference				Source		
ISS X-Force Database: quicktime-content-header-bo (8126): QuickTime `Content-Type` header buffer overflow				af854a3a-2127-422b-91ae-		
Apple QuickTime Content-Type Remote Buffer Overflow Vulnerability				af854a3a-2127-422b-91ae-		
'[SPSadvisory#46]Apple QuickTime Player "Content-Type" Buffer Overflow' - MARC				af854a3a-2127-422b-91ae-		
Apple QuickTime 7.2/7.3 RSTP Response Universal Exploit (win/osx)				af854a3a-2127-422b-91ae-		
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.						