CVE-2004-0387

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

Summary

CVE	CVE-2004-0387
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-06-01 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Stack-based buffer overflow in the RT3 plugin, as used in RealPlayer 8, RealOne Player, RealOne Player 10 beta, and Rea

Risk And Classification

Primary CVSS: v2.0 5.1 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Realnetworks	Realone Player	All	All	All	All

Application	Realnetworks	Realone Player	All	All	enterprise	All
Application	Realnetworks	Realone Player	10_beta	All	All	All
Application	Realnetworks	Realplayer	8.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
www.osvdb.org/displayvuln.php	af854a3a-2127-422b-91ae-364da2661108
archives.neohapsis.com/archives/vulnwatch/2004-q1/0077.html	af854a3a-2127-422b-91ae-364da2661108
'REAL One Player R3T File Format Stack Overflow' - MARC	af854a3a-2127-422b-91ae-364da2661108
Secunia - Advisories - RealPlayer/RealOne R3T File Handling Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108
www.ngssoftware.com/advisories/realr3t.txt	af854a3a-2127-422b-91ae-364da2661108
RealNetworks RealOne Player/RealPlayer Remote R3T File Stack Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108
404 Not Found	af854a3a-2127-422b-91ae-364da2661108
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108
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.