



CVE-2007-3410

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2007-3410
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-06-26 22:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Stack-based buffer overflow in the SmilTimeValue::parseWallClockValue function in smlprstime.cpp in RealNetworks RealF

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Realnetworks	Helix Player	10.0.5	All	All	All

Application	Realnetworks	Helix Player	10.0.6	All	All	All
Application	Realnetworks	Helix Player	10.0.7	All	All	All
Application	Realnetworks	Helix Player	10.0.8	All	All	All
Application	Realnetworks	Helix Player	10.5-gold	All	All	All
Application	Realnetworks	Realone Player	All	All	All	All
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.1	All	All	All
Application	Realnetworks	Realplayer	10.5	All	All	All
Application	Realnetworks	Realplayer Enterprise	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
Gentoo update for realplayer - Advisories - Secunia	af854a3a-2127-422
Repository / Oval Repository	af854a3a-2127-422
rhn.redhat.com Red Hat Support	af854a3a-2127-422
IBM X-Force Exchange	af854a3a-2127-422
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422
RealPlayer/RealOne/HelixPlayer Multiple Buffer Overflows - Advisories - Secunia	af854a3a-2127-422
RealPlayer/HelixPlayer ParseWallClockValue Function Buffer Overflow Vulnerability	af854a3a-2127-422
[VIM] RealPlayer Updates of October 25, 2007	af854a3a-2127-422
osvdb.org/38342	af854a3a-2127-422
RealPlayer SMIL parseWallClockValue() Stack Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422
osvdb.org/37374	af854a3a-2127-422
US-CERT Vulnerability Note VU#770904	af854a3a-2127-422
Webmail - OVH	af854a3a-2127-422
Helix Player SMIL parseWallClockValue() Stack Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422
labs.idefense.com/intelligence/vulnerabilities/display.php	af854a3a-2127-422
Red Hat update for RealPlayer - Advisories - Secunia	af854a3a-2127-422
RealPlayer and StarSearch by Real Official Homepage — Real.com	af854a3a-2127-422
RealPlayer/Helix Player SMIL wallclock Buffer Overflow Vulnerability - Advisories - Secunia	af854a3a-2127-422
rhn.redhat.com Red Hat Support	af854a3a-2127-422
RealPlayer: Buffer overflow — Gentoo Linux Documentation	af854a3a-2127-422
Red Hat update for HelixPlayer - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422

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.

© [CVE.report](#) 2026 |

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 registered 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)