



CVE-2004-1094

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2004-1094
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-10 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in InnerMedia DynaZip DUNZIP32.dll file version 5.00.03 and earlier allows remote attackers to execute arb

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Checkmark	Checkmark Payroll	3.7.5	All	All	All

Application	Checkmark	Checkmark Payroll	3.9.1	All	All	All
Application	Checkmark	Checkmark Payroll	3.9.2	All	All	All
Application	Checkmark	Checkmark Payroll	3.9.3	All	All	All
Application	Checkmark	Checkmark Payroll	3.9.4	All	All	All
Application	Checkmark	Checkmark Payroll	3.9.5	All	All	All
Application	Checkmark	Checkmark Payroll	All	All	All	All
Application	Checkmark	Multiledger	6.0.3	All	All	All
Application	Checkmark	Multiledger	6.0.5	All	All	All
Application	Checkmark	Multiledger	7.0.0	All	All	All
Application	Checkmark	Multiledger	All	All	All	All
Application	Innermedia	Dynazip Library	5.00.00	All	All	All
Application	Innermedia	Dynazip Library	5.00.01	All	All	All
Application	Innermedia	Dynazip Library	5.00.02	All	All	All
Application	Innermedia	Dynazip Library	5.00.03	All	All	All
Application	Realnetworks	Realone Player	1.0	All	All	All
Application	Realnetworks	Realone Player	2.0	All	All	All
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.0_6.0.12.690	All	All	All
Application	Realnetworks	Realplayer	10.0_beta	All	All	All
Application	Realnetworks	Realplayer	10.5	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1016_beta	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1040	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1053	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
This domain name is registered with Netim	af8:
Customer Support - Real Security Updates	af8:
SecuriTeam - CheckMark MultiLedger Buffer Overflow Vulnerability (DUNZIP32.dll)	af8:
'High Risk Vulnerability in RealPlayer' - MARC	af8:
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af8:
CheckMark Payroll DUNZIP32.dll Buffer Overflow Vulnerability - Advisories - Secunia	af8:
SecurityTracker.com Archive - RealPlayer Skin File Buffer Overflow May Let Remote Users Run Arbitrary Code	af8:

SecurityTracker.com Archives - RealPlayer Skin File Buffer Overflow may Let Remote Users Run Arbitrary Code	af8:
US-CERT Vulnerability Note VU#582498	af8:
Neohapsis Archives - Full Disclosure List - #1044 - [Full-Disclosure] EEYE: RealPlayer Zipped Skin File Buffer Overflow	af8:
SecurityTracker.com Archives - DynaZip Buffer Overflow in Processing Long Filenames May Let Remote Users Execute Arbitrary Code	af8:
This domain name is registered with Netim	af8:
This domain name is registered with Netim	af8:
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af8:
This domain name is registered with Netim	af8:
Secunia - Advisories - McAfee VirusScan DUNZIP32.dll Buffer Overflow Vulnerability	af8:
InnerMedia DynaZip Remote Stack Based Buffer Overflow Vulnerability	af8:
SecurityFocus	af8:
IBM Lotus Notes Buffer Overflow in 'DUNZIP32.dll' Lets Remote Users Execute Arbitrary Code - SecurityTracker	af8:
IBM X-Force Exchange	af8:
dtSearch DUNZIP32.dll Buffer Overflow Vulnerability - Advisories - Secunia	af8:
SecurityReason - dtSearch DUNZIP32.dll Buffer Overflow Vulnerability	af8:
SecurityFocus	af8:
Secunia - Advisories - CheckMark MultiLedger DUNZIP32.dll Buffer Overflow Vulnerability	af8:
SecurityFocus	af8:
This domain name is registered with Netim	af8:
SecurityReason	af8:
www.osvdb.org/19906	af8:
IBM X-Force Exchange	af8:
CVE Program record	CVI
NVD vulnerability detail	NVI

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](#)

