



CVE-2009-1351

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

Summary

CVE	CVE-2009-1351
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-21 16:24:00 UTC
Updated	2017-09-29 01:34:00 UTC
Description	Heap-based buffer overflow in Apollo 37zz allows remote attackers to cause a denial of service (application crash) and pos

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Heikki Ylinen	Apollo	37zz	All	All	All
Application	Heikki Ylinen	Apollo	37zz	All	All	All

References

Reference	Source
53770	OSVDB
Apollo 37zz Playlist Processing Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Apollo 'm3u' Playlist File Heap Buffer Overflow Vulnerability	BID
Apollo 37zz (M3u File) Local Heap Overflow PoC	EXPLOIT-DB
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](#)