



CVE-2009-4097

Published on: 11/28/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:23 PM UTC

CVE-2009-4097

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Serenity Audio Player](#) from [Malsmith](#) contain the following vulnerability:

Stack-based buffer overflow in the MplayInputFile function in Serenity Audio Player 3.2.3 and earlier allows remote attackers to execute arbitrary code via a long URL in an M3U file. NOTE: some of these details are obtained from third party information.

CVE-2009-4097 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Serenity "MplayInputFile()" M3U Playlist Buffer Overflow - Secunia Advisories - Vulnerability Information - Secunia.com

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[X SECUNIA 37472](#)

Files ~ Packet Storm

[Exploit](#)
[packetstormsecurity.org](#)
[text/x-python](#)

[MISC](#)
[packetstormsecurity.org/0911-exploits/serenityaudio-overflow.txt](#)

Serenity Audio Player Playlist (.m3u) BOF

[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 10226](#)

No Description Provided

[osvdb.org](#)

[OSVDB 60503](#)

Inactive Link **Not Archived**

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Malsmith	Serenity Audio Player	3.0.1	All	All	All
Application	Malsmith	Serenity Audio Player	3.0.2	All	All	All
Application	Malsmith	Serenity Audio Player	3.2.0	All	All	All
Application	Malsmith	Serenity Audio Player	3.2.1	All	All	All
Application	Malsmith	Serenity Audio Player	3.2.2	All	All	All
Application	Malsmith	Serenity Audio Player	3.0.1	All	All	All
Application	Malsmith	Serenity Audio Player	3.0.2	All	All	All
Application	Malsmith	Serenity Audio Player	3.2.0	All	All	All
Application	Malsmith	Serenity Audio Player	3.2.1	All	All	All
Application	Malsmith	Serenity Audio Player	3.2.2	All	All	All
Application	Malsmith	Serenity Audio Player	All	All	All	All
cpe:2.3:a:malsmith:serenity_audio_player:3.0.1:*****:.*:						
cpe:2.3:a:malsmith:serenity_audio_player:3.0.2:*****:.*:						
cpe:2.3:a:malsmith:serenity_audio_player:3.2.0:*****:.*:						
cpe:2.3:a:malsmith:serenity_audio_player:3.2.1:*****:.*:						
cpe:2.3:a:malsmith:serenity_audio_player:3.2.2:*****:.*:						
cpe:2.3:a:malsmith:serenity_audio_player:3.0.1:*****:.*:						
cpe:2.3:a:malsmith:serenity_audio_player:3.0.2:*****:.*:						
cpe:2.3:a:malsmith:serenity_audio_player:3.2.0:*****:.*:						
cpe:2.3:a:malsmith:serenity_audio_player:3.2.1:*****:.*:						
cpe:2.3:a:malsmith:serenity_audio_player:3.2.2:*****:.*:						
cpe:2.3:a:malsmith:serenity_audio_player:*****:.*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID→](#)

© [CVE.report](#) 2023   |

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](#).

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