



CVE-2008-0959

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

Summary

CVE	CVE-2008-0959
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-05-29 16:32:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Multiple stack-based buffer overflows in the Online Media Technologies NCTSoft NCTAudioInformation2 ActiveX control in

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Alivemedia	Alive Mp3 Wav Converter	3.9.3.2	All	All	All

Application	Online Media Technologies	Nctaudioeditor Activex Control	All	All	All	All
Application	Online Media Technologies	Nctaudiostudio Activex Control	All	All	All	All
Application	Orion Studios	Cinematicmp3	1.4.0.0	All	All	All
Application	Ussun	Power Audio Cd Burner	1.02	All	All	All
Application	Ussun	Power Audio Cd Grabber	1.0	All	All	All

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

References
Reference
VU#669265 - Online Media Technologies NCTSoft NCTAudioInformation2 ActiveX stack buffer overflows
Alive MP3 WAV Converter NCTAudioInformation2.dll ActiveX Control Buffer Overflow - Secunia Advisories - Vulnerability Intelligence - Secunia
Audio Editor Plus NCTAudioInformation2.dll ActiveX Control Buffer Overflow - Advisories - Secunia
Powerful Audio Tool NCTAudioInformation2.dll ActiveX Control Buffer Overflow - Advisories - Secunia
Power Audio CD Burner NCTAudioInformation2 ActiveX Control Buffer Overflow - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
4U WMA MP3 Converter NCTAudioInformation2.dll ActiveX Control Buffer Overflow - Advisories - Community
Total Audio Recorder and Editor NCTSoft ActiveX Controls Buffer Overflow Vulnerabilities - Advisories - Secunia
Easy Audio Redactor NCTSoft ActiveX Controls Buffer Overflow Vulnerabilities - Advisories - Secunia
Crystal MP3 Recorder NCTAudioInformation2.dll ActiveX Control Buffer Overflow - Advisories - Secunia
CinematicMP3 NCTAudioInformation2 ActiveX Control Buffer Overflow - Advisories - Secunia
IBM X-Force Exchange
My Phone Files Media Studio NCTSoft ActiveX Controls Buffer Overflow Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia
Power Audio CD Grabber NCTAudioInformation2 ActiveX Control Buffer Overflow - Advisories - Secunia
Total Audio Capture NCTAudioInformation2.dll ActiveX Control Buffer Overflow - Advisories - Secunia
NCTSoft Products NCTAudioInformation2 ActiveX Control Buffer Overflows - Secunia Advisories - Vulnerability Intelligence - Secunia.com
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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