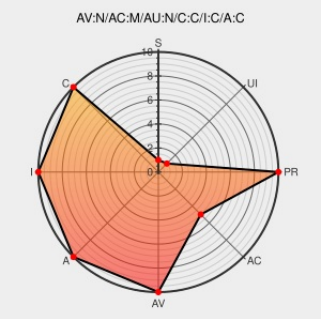
CVE-2009-3812

Published on: 10/27/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:24 PM UTC

CVE-2009-3812

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Otsav Dj from Otslabs contain the following vulnerability:

Heap-based buffer overflow in OtsAV DJ trial version 1.85.64.0, Radio trial version 1.85.64.0, TV trial version 1.85.64.0, and Free version 1.77.001 allows remote attackers to execute arbitrary code via a long playlist in an Ots File List (.ofl) file.

CVE-2009-3812 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF otsav-multiple-olf-bo(51628)
OtsAV Products Ots File List Processing Buffer Overflow - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 35738
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2009-1861
otsAV DJ/TV/Radio - Multiple Local Heap Overflows (PoC) - Windows dos Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 9113
No Description Provided	osvdb.org	OSVDB 55747

	Inactive Link Not Archived	
Files ≈ Packet Storm	Exploit packetstormsecurity.org text/plain	MISC packetstormsecurity.org/0907-exploits/otsav-overflow.txt

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	Otslabs	Otsav Dj	1.85.64.0	trial	All	All
Application	Otslabs	Otsav Dj	1.85.64.0	trial	All	All
Application	Otslabs	Otsav Radio	1.85.64.0	trial	All	All
Application	Otslabs	Otsav Radio	1.85.64.0	trial	All	All
Application	Otslabs	Otsav Tv	1.85.64.0	trial	All	All
Application	Otslabs	Otsav Tv	1.85.64.0	trial	All	All

cpe:2.3:a:otslabs:otsav_dj:1.85.64.0:trial:*:*:*:*:*:*:

cpe:2.3:a:otslabs:otsav_dj:1.85.64.0:trial:*:*:*:*:*:*:

cpe:2.3:a:otslabs:otsav_radio:1.85.64.0:trial:*:*:*:*:*:*:

cpe:2.3:a:otslabs:otsav_radio:1.85.64.0:trial:*:*:*:*:*:*:

cpe:2.3:a:otslabs:otsav_tv:1.85.64.0:trial:*:*:*:*:*:*:

cpe:2.3:a:otslabs:otsav_tv:1.85.64.0:trial:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→