



CVE-2012-3941

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

Summary

CVE	CVE-2012-3941
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-10-25 14:55:00 UTC
Updated	2013-05-04 03:20:00 UTC
Description	Heap-based buffer overflow in the Cisco WebEx Recording Format (WRF) player T27 before LD SP32 EP10 and T28 before

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Webex Recording Format Player	27.11.26	All	All	All
Application	Cisco	Webex Recording Format Player	27.21.10	All	All	All
Application	Cisco	Webex Recording Format Player	27.25.10	All	All	All
Application	Cisco	Webex Recording Format Player	27.32.1	All	All	All
Application	Cisco	Webex Recording Format Player	28.0.0	All	All	All
Application	Cisco	Webex Recording Format Player	27.11.26	All	All	All
Application	Cisco	Webex Recording Format Player	27.21.10	All	All	All
Application	Cisco	Webex Recording Format Player	27.25.10	All	All	All
Application	Cisco	Webex Recording Format Player	27.32.1	All	All	All
Application	Cisco	Webex Recording Format Player	28.0.0	All	All	All

References

Reference	Source	Link
Cisco WebEx Player Buffer Overflows Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTrack	www.securitytracker.com
86140	OSVDB	osvdb.org
Cisco WebEx WRF File Format Multiple Remote Memory Corruption Vulnerabilities	BID	www.securityfocus.com
Cisco Security Advisory: Multiple Vulnerabilities in the Cisco WebEx Recording Format Player	CISCO	tools.cisco.com

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
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