



CVE-2011-0354

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

Summary

CVE	CVE-2011-0354
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-03 16:00:00 UTC
Updated	2011-09-22 03:28:00 UTC
Description	The default configuration of Cisco Tandberg C Series Endpoints, and Tandberg E and EX Personal Video units, with software

Risk And Classification

Problem Types: CWE-255

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Tandberg Endpoint	tc2.1.2	All	All	All
Application	Cisco	Tandberg Endpoint	tc3.0.0	All	All	All
Application	Cisco	Tandberg Endpoint	tc3.1.0	All	All	All
Application	Cisco	Tandberg Endpoint	tc3.1.1	All	All	All
Application	Cisco	Tandberg Endpoint	tc3.1.2	All	All	All
Hardware	Cisco	Tandberg Endpoint	c20	All	All	All
Hardware	Cisco	Tandberg Endpoint	c40	All	All	All
Hardware	Cisco	Tandberg Endpoint	c60	All	All	All
Hardware	Cisco	Tandberg Endpoint	c90	All	All	All
Application	Cisco	Tandberg Endpoint	tc2.1.2	All	All	All
Application	Cisco	Tandberg Endpoint	tc3.0.0	All	All	All
Application	Cisco	Tandberg Endpoint	tc3.1.0	All	All	All
Application	Cisco	Tandberg Endpoint	tc3.1.1	All	All	All
Application	Cisco	Tandberg Endpoint	tc3.1.2	All	All	All
Hardware	Cisco	Tandberg Endpoint	c20	All	All	All
Hardware	Cisco	Tandberg Endpoint	c40	All	All	All
Hardware	Cisco	Tandberg Endpoint	c60	All	All	All

Hardware	Cisco	Tandberg Endpoint	c90	All	All	All
Application	Cisco	Tandberg Endpoint	All	All	All	All
Hardware	Cisco	Tandberg Personal Video Unit	e20	All	All	All
Hardware	Cisco	Tandberg Personal Video Unit	ex60	All	All	All
Hardware	Cisco	Tandberg Personal Video Unit	ex90	All	All	All
Hardware	Cisco	Tandberg Personal Video Unit	e20	All	All	All
Hardware	Cisco	Tandberg Personal Video Unit	ex60	All	All	All
Hardware	Cisco	Tandberg Personal Video Unit	ex90	All	All	All
Application	Cisco	Tandberg Personal Video Unit Software	tc3.1.0	All	All	All
Application	Cisco	Tandberg Personal Video Unit Software	tc3.1.1	All	All	All
Application	Cisco	Tandberg Personal Video Unit Software	tc3.1.2	All	All	All
Application	Cisco	Tandberg Personal Video Unit Software	te1.0.1	All	All	All
Application	Cisco	Tandberg Personal Video Unit Software	te2.2.0	All	All	All
Application	Cisco	Tandberg Personal Video Unit Software	tc3.1.0	All	All	All
Application	Cisco	Tandberg Personal Video Unit Software	tc3.1.1	All	All	All
Application	Cisco	Tandberg Personal Video Unit Software	tc3.1.2	All	All	All
Application	Cisco	Tandberg Personal Video Unit Software	te1.0.1	All	All	All
Application	Cisco	Tandberg Personal Video Unit Software	te2.2.0	All	All	All
Application	Cisco	Tandberg Personal Video Unit Software	All	All	All	All
Application	Cisco	Tandberg Personal Video Unit Software	All	All	All	All

References						
Reference					Source	
Tandberg E, EX and C Series Endpoints Default Credentials for Root Account - CXSecurity.com					SREASON	
Cisco TANDBERG C Series and E/EX Series Default Credentials Authentication Bypass Vulnerability					BID	
Alert Details - Security Center - Cisco Systems					CONFIRM	
Cisco Security Advisory: Default Credentials for Root Account on Tandberg E, EX and C Series Endpoints - Cisco Systems					CISCO	
US-CERT Vulnerability Note VU#436854 - Cisco Tandberg E, EX, and C Series default root credentials					CERT-VN	
TANDBERG Products Root Default Password Security Issue - Secunia.com					SECUNIA	
Tandberg E, EX and C Series Endpoints Default Credentials for Root Account					EXPLOIT-DB	
TANDBERG Videoconferencing Systems Default Account Lets Remote Users Gain Root Access - SecurityTracker					SECTrack	
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](#)