



CVE-2010-1355

Published on: 04/13/2010 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:05:00 AM UTC

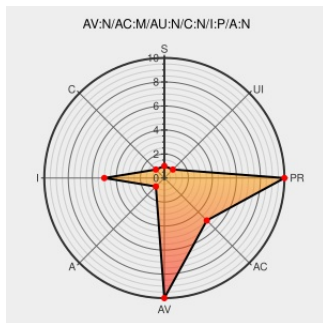
CVE-2010-1355

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Tandberg Video Communication Server](#) from [Vsecurity](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability on the TANDBERG Video Communication Server (VCS) before X5.0 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka Reference ID 66316.

CVE-2010-1355 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

TelePresence
- Cisco
Systems

[ftp.tandberg.com](#)
[text/html](#)

[CONFIRM](#)

[ftp.tandberg.com/pub/software/vcs/TANDBERG%20Video%20Communication%20Server%20Software%2](#)

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	Vsecurity	Tandberg Video Communication Server	x1.0.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x1.1.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x1.2.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x2.0.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x2.1.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x3.0.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x3.1.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x4.1.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x4.2.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x4.2.1	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x1.0.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x1.1.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x1.2.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x2.0.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x2.1.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x3.0.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x3.1.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x4.1.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x4.2.0	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	x4.2.1	All	All	All
Application	Vsecurity	Tandberg Video Communication Server	All	All	All	All
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x1.0.0:****:****:						
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x1.1.0:****:****:						
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x1.2.0:****:****:						
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x2.0.0:****:****:						
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x2.1.0:****:****:						
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x3.0.0:****:****:						
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x3.1.0:****:****:						
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x4.1.0:****:****:						
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x4.2.0:****:****:						
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x4.2.1:****:****:						

cpe:2.3:a:vsecurity:tandberg_video_communication_server:x1.0.0:~::~::~::~:
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x1.1.0:~::~::~::~:
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x1.2.0:~::~::~::~:
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x2.0.0:~::~::~::~:
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x2.1.0:~::~::~::~:
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x3.0.0:~::~::~::~:
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x3.1.0:~::~::~::~:
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x4.1.0:~::~::~::~:
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x4.2.0:~::~::~::~:
cpe:2.3:a:vsecurity:tandberg_video_communication_server:x4.2.1:~::~::~::~:
cpe:2.3:a:vsecurity:tandberg_video_communication_server:~::~::~::~:

No vendor comments have been submitted for this CVE