

# Cisco Security Response: Cisco TelePresence Video Communication Server Cross-Site Scripting Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sr-20111012-vcs.shtml>

## Revision 1.0

For Public Release 2011 October 12 1730 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

[Cisco Response](#)  
[Additional Information](#)  
[Status of this Notice: FINAL](#)  
[Revision History](#)  
[Cisco Security Procedures](#)

---

## Cisco Response

A vulnerability exists in Cisco TelePresence Video Communication Server (VCS) due to improper validation of user-controlled input to the web-based administrative interface. User-controlled input supplied to the login page via the HTTP User-Agent header is not properly sanitized for illegal or malicious content prior to being returned to the user in dynamically generated web content. A remote attacker could exploit this vulnerability to perform reflected cross-site scripting attacks.

Billy Hoffman from Zoompf, Inc., discovered this vulnerability and Ben Feinstein from Dell SecureWorks reported it to Cisco. Cisco greatly appreciates the opportunity to work with researchers on security vulnerabilities and welcome the opportunity to review and assist in product reports.

## Additional Information

Cisco TelePresence Video Communication Server Software versions earlier than X7.0 are affected. This vulnerability has been corrected in Cisco TelePresence Video Communication Server Software version X7.0.

This vulnerability is documented in Cisco bug ID [CSCts80342](#) ([registered](#) customers only) and has been assigned CVE ID CVE-2011-3294.

Additional mitigations that can be deployed on Cisco devices in the network are available in the Cisco Applied Mitigation Bulletin: Understanding Cross-Site Scripting (XSS) Threat Vectors: <http://www.cisco.com/warp/public/707/cisco-amb-20060922-understanding-xss.shtml>

## Status of this Notice: FINAL

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

## Revision History

Revision 1.0	2011-October-12	Initial public release
--------------	-----------------	------------------------

## Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

**Suggestions for improvement:**

(256 character limit)

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 - 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)