Tandberg Video Communications Server Cross-Site Scripting (XSS) Vulnerability

Dell SecureWorks Security Advisory SWRX-2011-003

Advisory Information

Title: Tandberg Video Communications Server Cross-Site Scripting (XSS) Vulnerability
Advisory ID: SWRX-2011-003
Advisory URL: http://www.secureworks.com/research/advisories/SWRX-2011-003/
Date published: Wednesday, October 12, 2011
CVE: CVE-2011-3294
CVSS v2 Base Score: 4.3
Date of last update: Wednesday, October 12, 2011
Vendors contacted: Cisco Systems, Inc.
Release mode: Coordinated
Discovered by: Billy Hoffman, Zoompf, Inc.

Summary

A vulnerability exists in Tandberg Video Communications 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 (XSS) attacks.

Affected Products

Tandberg Video Communications Server prior to version X7.0.

Cisco has rebranded the Tandberg Video Communications Server product as Cisco TelePresence Video Communication Server.

http://www.tandberg.com/video-conferencing-network-infrastructure/video-communication-server.jsp

Vendor Information, Solutions and Workarounds

The vulnerability has been addressed with Cisco Bug ID CSCts80342

Cisco's vendor response can be found at http://www.cisco.com/warp/public/707/cisco-sr-20111012-vcs.shtml

Details

The Tandberg Video Communications Server provides call control and interoperability for enterprise telepresence and video conferencing. From the vendor's description: "The Video Communications Server (VCS) provides the most advanced telepresence and video conferencing call control in the industry. It enables any-to-any interoperability between all standards-compliant SIP and H.323 devices."[1]

The Tandberg Video Communications Server fails to properly validate 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. The login page reflects the HTTP User-Agent header in an HTML comment located at the bottom of the returned page.

Figure 1. Source of VCS login page, illustrating reflection of the HTTP User-Agent header within an HTML comment.

[1] http://www.tandberg.com/video-conferencing-network-infrastructure/video-communication-server.jsp

Cross-site scripting vulnerabilities due to an unsanitized reflected HTTP header are typically more difficult to exploit in practice because the attacker has little control over the HTTP headers sent by the victim's web browser. However, the HTTP User-Agent header can sometimes be controlled through browser plug-ins such as Adobe Flash, Java applets, or AJAX.

CVSS Severity (version 2.0)

Access Vector: Network
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Cross-Site Scripting
Confidentiality Impact: None
Integrity Impact: Partial
Availability Impact: None
CVSS v2 Base Score: 4.3
CVSS v2 Impact Subscore: 2.9
CVSS v2 Exploitability Subscore: 8.6
CVSS v2 Vector: (AV:N/AC:M/Au:N/C:N/I:P/A:N)

Proof of Concept

By using a specially crafted HTTP User-Agent header, such as

```
User-Agent: Mozilla/5.0 --><script>alert('XSS Discovered by
Zoompf');</script><!--
```

an attacker can execute a reflected cross-site scripting attack as shown below.

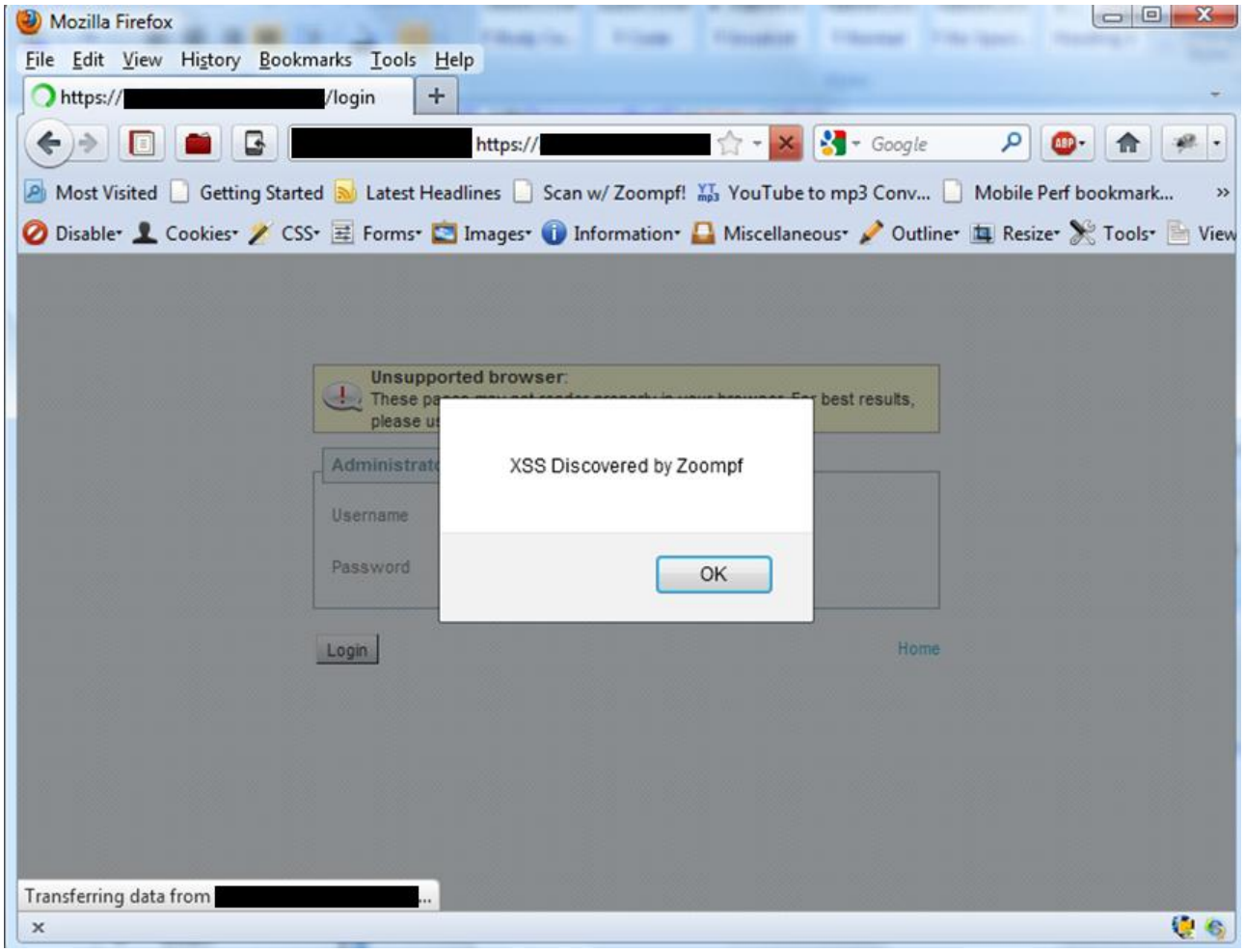

Figure 2. JavaScript alert message in web browser, illustrating successful exploitation of reflected cross-site scripting vulnerability in VCS.

Revision History

1.0 2011-10-12 – Initial advisory release

PGP Keys

This advisory has been signed with the Dell SecureWorks Counter Threat Unit℠ PGP key, which is available for download at http://www.secureworks.com/contact/SecureWorksCTU.asc.

About Dell SecureWorks

Dell focuses exclusively on security services to protect more than 2,900 clients around the world. Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help

organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

Disclaimer