

TANDBERG

**VCS X2.0 Security
Advisory**

D50529 Revision 1.0

May 2008

TABLE OF CONTENTS

TANDBERG VCS X2.0 SECURITY ADVISORY	4
Introduction	4
Web Proxy Vulnerability	4
<i>Overview of Vulnerability</i>	4
<i>Current Resolutions</i>	4

DOCUMENT REVISION HISTORY

Revision 1.0 Initial version

TANDBERG VCS X2.0 SECURITY ADVISORY

Introduction

TANDBERG has discovered a security vulnerability with the TANDBERG Video Communication Server (VCS), introduced within the X2.0 release of software. This document will discuss the security vulnerability as well as potential short term and long term resolutions to the issues.

Web Proxy Vulnerability

Overview of Vulnerability

Within the X2.0 software release, an issue was introduced, allowing an attacker to utilize the VCS to re-direct web requests outside of the box to a remote server, essentially utilizing the web server on the VCS as a proxy to other addresses within the space. This issue is specific to the web server on the TANDBERG VCS and does not affect the operation or security of any of the H.323, SIP or traversal functionality.

Note: This issue does **not** affect the security provided by the Expressway technology as any of the traffic that would be re-directed by the proxy vulnerability would never enter into this connection. Any re-direction of traffic would remain on the same network segment on which the VCS resides and would be subject to the same network policies and rules that are afforded to the VCS management traffic.

Severity

The severity of this issue is considered to be low due to the fact that only the web interface of the box is affected. The traversal, H.323 and SIP functionality is neither affected nor compromised by the vulnerability.

TANDBERG does recommend all customers take action through one of the proposed solutions below to prevent any issues from arising from the vulnerability.

Affected Systems

All TANDBERG VCS products with HTTP and/or HTTPS 'Enabled' and running X2.0 software are affected by the web proxy vulnerability.

Current Resolutions

Disable HTTP(S)

The vulnerability explicitly affects the HTTP and HTTPS remote management interfaces. If these interfaces are either disabled or access to these interfaces is prevented through firewall and/or security policies on the network.

Disable Proxy on X2.0 VCS

It is possible to issue commands to the TANDBERG VCS to disable this security vulnerability. Please contact your TANDBERG Service Representative for more information regarding this procedure.

Firewall Remote Management

TANDBERG recommends, as a best practice, to place externally facing VCS boxes within a portion of the network interface that prevents potential attackers outside the network from accessing the VCS over

the remote management interfaces. For deployments within this model, the web proxy vulnerability, as addressed above, does not pose a large threat to those networks.

Downgrade to X1.2

The web proxy issue was introduced within the X2.0 release of software. Therefore, any version previous to X2.0 does not exhibit the issue and can be safely loaded onto any production-level VCS boxes to prevent this issue from occurring.

Note: TANDBERG has verified the downgrade procedure of the VCS from X2.0 to X1.2 does not encounter any major issues with the parameter restoration.

Upgrade to X2.1

The proxy vulnerability has already been addressed in a release candidate version of X2.1, X2.1RC2. This release candidate, while beta software, is considered a stable release of software and can be loaded on production-grade VCS products within the customer market, pending a final upgrade to X2.1 when released to the market. The current plan of record for the X2.1 final release is to be out to the market by late May or early June 2008.

Note: While the software is considered stable and a valid release for use within a production environment, precautions should be taken whenever upgrading infrastructure hardware to a beta version of software. No major issues are expected with the X2.1RC2 version of software; however, there are no guarantees that the software does not contain issues that could affect the operation of the software. Additionally, this release candidate version of X2.1 is provided without any documentation or release notes that document what has changed as the software still is in beta form. Upon release of X2.1 final version of software to the market, release notes and documentation will be provided containing this information.