

Cisco Security Response: VoIPshield Reported Vulnerabilities in Cisco Unity Server

<http://www.cisco.com/warp/public/707/cisco-sr-20081008-unity.shtml>

Revision 1.0

For Public Release 2008 October 8 1800 UTC (GMT)

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

Contents

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is the Cisco PSIRT response to the vulnerabilities in Cisco Unity by VoIPshield, in their recent advisories (VSRCS-2008-008 to VSRCS-2008-012). The original advisories are available at:

www.voipshield.com .

The Cisco PSIRT team greatly appreciates the opportunity to work with researchers on security vulnerabilities, and we welcome the opportunity to review and assist in product reports. We thank VoIPshield for reporting this vulnerability to Cisco PSIRT.

Workarounds and code level fixes are provided in the following sections.

VSRCS-2008-008: Cisco Unity Authentication Bypass

Cisco has issued a security advisory on this issue.

It is available at: <http://www.cisco.com/warp/public/707/cisco-sa-20081008-unity.shtml>

VSRCs-2008-009: Cisco Unity Stored Cross Site Scripting Vulnerability

Cisco acknowledges this vulnerability and has made improvements on the front end and back end mitigations for cross site scripting attacks.

This particular vulnerability requires an authenticated administrator to enter malicious data into the database.

This vulnerability is documented in Cisco Bug ID [CSCsr86345](#) ([registered](#) customers only) .

Fixed Software

This vulnerability will be fixed in the following Cisco Unity releases:

- 4.2(1)ES162
- 5.0(1)ES56
- 7.0(2)ES8

Workaround

There is no workaround for this vulnerability. Use strong passwords for administrator accounts.

VSRCs-2008-010: Cisco Unity Session Exhaustion Denial of Service

Cisco acknowledges this vulnerability and has made fixed software available.

This vulnerability only affects Cisco Unity servers configured to use anonymous authentication as described in the Installation Guide for Cisco Unity in the [Authentication Methods Available for the Cisco Unity Administrator](#) section. This vulnerability is documented in Cisco Bug ID [CSCsr86971](#) ([registered](#) customers only) .

Fixed Software

This vulnerability is fixed in the following Cisco Unity releases:

- 4.2(1)ES161
- 5.0(1)ES53
- 7.0(2)ES8

Workaround

Administrators can change the number of SA sessions available by changing the following registry key:

```
\HKLC\Software\Active Voice\SystemParams\1.0\SaSessions
```

VSRCs-2008-011

Cisco acknowledges this vulnerability. Fixed software will be included in an upcoming Windows update.

This vulnerability is the result of a processing error in a Microsoft API used by Cisco Unity. Cisco and Microsoft have jointly investigated this issue and Microsoft will provide a fix as soon as possible. Cisco is tracking this issue with the bug [CSCsr86990](#) ([registered](#) customers only) .

Fixed Software

This vulnerability will be fixed in an upcoming Microsoft Windows update.

Workaround

None.

VSRCs-2008-012

Cisco acknowledges this vulnerability and has made improvements during new installations of Cisco Unity. Current Cisco Unity users should follow the workaround provided below. This vulnerability is documented in Cisco Bug ID [CSCsr86983](#) ([registered](#) customers only) .

Fixed Software

This vulnerability is fixed in the following Cisco Unity releases:

- 4.2(1)ES161
- 5.0(1)ES53
- 7.0(2)ES8

Workaround

Manually remove read permissions for domain users on D:\CommServer\Reports. This can be done by right clicking the directory in the Windows Explorer, selecting properties, then under the Sharing tab, clicking the Permissions button. Read access for domain users can safely be disabled and will not be the default configuration in future Cisco Unity installations.

Additional Information

The fixed software mentioned in this response is available at:

- [4.2\(1\) ES releases](#)
- [5.0\(1\) ES releases](#)
- [7.0\(2\) ES releases](#)

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.

Revision History

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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories and responses 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)