

Cisco Security Advisory: Predefined Restriction Tables Allow Calls to International Operator

Document ID: 27663

Advisory ID: cisco-sa-20021004-toll-fraud

<http://www.cisco.com/warp/public/707/cisco-sa-20021004-toll-fraud.shtml>

Revision 1.1

Last Updated 2002 October 05 0130 UTC (GMT)

For Public Release 2002 October 04 1530 UTC (GMT)

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

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of This Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

The predefined restriction tables in Cisco Unity do not block calls to the international operator. The default configuration only blocks North American Numbering Plan (NANP) International Direct Dial (IDD) prefixes, or those prefixes that start with 9 011. Customers may expect that since direct dial international calls are blocked, it is not possible for users to forward calls to international numbers, but the loophole of the international operator is still allowed under the predefined restriction table. This subversion can be accomplished by anyone inside or outside of a company who is familiar with how to configure Cisco Unity and has access to a valid system username and password, which is further compounded by the common existence of the Example Administrator and Example Subscriber accounts in many installations.

This vulnerability has been documented as CSCdy54570. These issues are also being referenced in the Mitre CVE as CAN-2002-1189 and CAN-2002-1190.

The following products are identified as affected by this vulnerability:

- Cisco Unity software versions 3.1.5 and lower including all 2.x versions.

Unless explicitly stated otherwise, all other Cisco products are not affected.

A workaround exists for this vulnerability which is detailed in the [Workarounds](#) section below.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20021004-toll-fraud.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

Cisco Unity software versions 3.1.5 and lower including all 2.x versions.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

The predefined restriction tables in Cisco Unity are for North American dial plans and do not block calls to the international operator. The default configuration only blocks IDD patterns that start with 9 011. This may pose a problem because subscribers can configure call forwarding in Cisco Unity to point to the international operator (9 00) and then place international calls.

After installing Unity, customers often ignore the Example Administrator and Example Subscriber accounts. These can be exploited by dialing into Cisco Unity, logging into the accounts with the default extension and password, and configuring it to call forward to the international operator or other toll number.

Two other scenarios in which this could happen are:

1. Internal users can set their own Cisco Unity mailboxes to forward to international numbers or toll numbers.
2. External callers could log into a poorly password protected mailbox (for example: password=1234), and forward to international numbers or toll numbers.

This vulnerability has been documented as CSCdy54570.

Impact

The predefined restriction tables within the Cisco Unity configuration allows direct dialing of the international operator or other toll calls which may not be desired. Due to the existence of well known default user accounts, successful exploitation of those default accounts or policies allowing weak passwords on accounts can result in toll fraud which may go unnoticed until the end of a billing cycle.

Software Versions and Fixes

The default configuration of Cisco Unity will be modified to disallow forwarding to the international operator in future versions, however a software upgrade is not necessary in order to mitigate the vulnerability.

Workarounds

Adding additional dial strings to the restriction tables will prevent Unity from trying to place a toll call. For example, to block all international calls as well as toll calls while still retaining the ability to dial locally, the following restriction table entries might be useful for installations in North America:

91??????*	No
90*	No
9????????	Yes
9???????	Yes

In the example above, the first line will match and block all domestic (US) toll calls. The second line will match and block all international calls including the international operator. The third line matches and allows local calls. This line is not necessary if your area does not use local area codes. The fourth line matches and allows local calls. This or other locally applicable lines should be applied to all restriction tables. Note that some locations use 10 digit dialing for non-toll calls. In those locations the restrictions should allow specific non-toll prefixes while blocking all other toll prefixes.

For installations outside of North America where the dial plans vary from the above example, the restriction table entries will be different. Information to assist in creating restriction tables can be found in the section entitled "Restriction Tables" in the Cisco Unity System Administration Guide.

In addition, Cisco recommends the protection of the Example Administrator and the Example Subscriber accounts. These accounts at a minimum should have their default extension and default password changed. This should be done as part of tightening the security on your Cisco Unity system. For more details refer to: [White Paper: Best Practices for Cisco Unity 3.0](#).

It is also possible to remove the Example Administrator and the Example Subscriber accounts. Care must be taken in removing the Example Administrator account, as removing it improperly could result in the Cisco Unity server no longer functioning properly. The process to remove those accounts has been documented at http://www.cisco.com/warp/public/788/AVVID/remove_example_admin.html.

Other methods of mitigating the risk are:

1. If Unity is integrated with a Call Manager, adding a route filter to the route pattern Unity uses to dial to the Public Switched Telephone Network (PSTN) will prevent calls to the international operator.
2. Restricting Unity from placing calls to the PSTN if that capability is not needed.
3. Apply a good password policy. Refer to the white paper on [Best Practices for Cisco Unity 3.0](#).

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

The Cisco PSIRT has been made aware of malicious use of the vulnerability described in this advisory. Customers are advised to perform the steps as described in the Workarounds section in order to prevent misuse of their Cisco Unity servers.

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.

Distribution

This notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20021004-toll-fraud.shtml>. In addition to Worldwide Web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients:

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com
- full-disclosure@lists.netsys.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

Future updates of this notice, if any, will be placed on Cisco's Worldwide Web server, but may or may not be actively announced on mailing lists or newsgroups.

Users concerned about this problem are encouraged to check the URL given above for any updates.

Revision History

Revision 1.1	2002–October–05	Updated to include specific release versions and added CVE numbers
Revision 1.0	2002–October–04	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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 05, 2002

Document ID: 27663
