

[Full-Disclosure] Cisco Security Advisory: Unity Vulnerabilities on IBM-based Servers

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-12/0398.html>

From: Cisco Systems Product Security Incident Response Team (*psirt_at_cisco.com*)

Date: 12/10/03

To: full-disclosure@lists.netsys.com

Date: Wed, 10 Dec 2003 09:00:00 -0800

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Cisco Security Advisory: Unity Vulnerabilities on IBM-based Servers

Revision Numeral 1.0

For Public Release 2003 December 10 17:00 UTC (GMT)

=====
Contents

=====
Summary
Affected Products
Details
Impact
Software Versions and Fixes
Obtaining Fixed Software
Workarounds
Exploitation and Public Announcements
Status of This Notice
Distribution
Revision History
Cisco Security Procedures
=====

=====
Summary

Recent installations of Cisco Unity running on IBM servers contain default user accounts and default IP addresses which should be removed or disabled immediately. Vulnerable systems can be identified by the part number on the installation disk or by following directions in the

Full-Disclosure: [Full-Disclosure] Cisco Security Advisory: Unity Vulnerabilities on IBM-based Servers

Workarounds section. Each vulnerability can be verified and removed manually without requiring an upgrade to new software or reinstallation. This vulnerability only applies to IBM-based Cisco Unity systems installed with specific part numbers on the installation disks. No other platforms running Cisco Unity are vulnerable.

This advisory will be available at

<http://www.cisco.com/warp/public/707/cisco-sa-20031210-unity.shtml>.

Affected Products

=====

IBM-based Cisco Unity servers purchased either as an MCS server or with direct IBM branding and installed with the Cisco Unity Server image disk supplied may be affected. Cisco Unity servers with the unintended local user account "bubba", default RAID Manager address, and default DHCP server address are affected. Following directions in the Workarounds section below, existence of each account or address can be verified.

Part numbers imprinted on the installation disks with a local user account "bubba", default RAID Manager address, and DHCP server address:

80-7111-01 for the UNITY-SVRX255-1A

80-7112-01 for the UNITY-SVRX255-2A

Part numbers imprinted on the installation disks with default RAID Manager address and DHCP server address (no local user account "bubba"):

80-6750-01 for the Unity SVRX232-1A

80-6765-01 for the UNITY-SVRX232-2A

80-7108-01 and 80-7108-02 for the UNITY-SVRX205-1A

80-7109-01 and 80-7109-02 for the UNITY-SVRX345-1A

80-7110-01 and 80-7110-02 for the UNITY-SVRX345-2A

80-7002-01 and 80-7003-01 for the UNITY-SVRX255-1A and UNITY-SVRX255-2A

80-7243-01 for the MCS-7815i-2.0-ECS1

80-7242-01 for the MCS-7835i-2.4-ECS1

80-7241-01 for the MCS-7845i-2.4-ECS1

80-7240-01 for the MCS-7845i-2.4-ECS2

80-7237-01 plus 80-7239-01 for the MCS-7855i-1.5-ECS1

80-7236-01 plus 80-7238-01 for the MCS-7855i-1.5-ECS2

80-7237-01 plus 80-7239-01 for the MCS-7865i-1.5-ECS1

80-7236-01 plus 80-7238-01 for the MCS-7865i-1.5-ECS2

Details

=====

Local User Account Issue

A local user account "bubba" with log on locally rights was created during manufacturing testing .

RAID Manager Issue

After installation, if the RAID (Redundant Array of Inexpensive Disks) Management service is configured to start automatically and not restricted to local-only, the service tries to establish a TCP session with a RAID server address which was used during testing at the manufacturer and leaves the TCP port 34571 open listening for remote contact. The TCP connection attempt is directed to an IP address embedded in the RaidNLst.ser file within the C:\Program Files\RaidMan directory. This is a configuration file which directs how and to whom Notification messages are sent for the RAID Management service (RaidServ.exe).

DHCP Issue

After installation, if the Cisco Unity Server is configured to get an IP address from a DHCP server and no local server exists, it will repeatedly send packets attempting to get an IP address from the DHCP server on the manufacturer's test network. The manufacturer's DHCP server IP address will remain in the registry until a local DHCP server is identified or a static entry is made for a local DHCP server.

Impact

Local User Account Issue

An unplanned local user account with log on locally rights leaves the system open to remote login, which may increase the risk of system compromise and unauthorized administrative access.

RAID Manager Issue

The RAID Management service attempts to connect to a RAID server on the manufacturer's test network and leaves the Cisco Unity Server listening on port 34571 to incoming TCP connections. The Cisco Unity Server is attempting to connect to a RAID server with a routable TCP/IP address that, as of the initial publication of this advisory, does not respond to pings or connection requests on the Internet, but good security practices suggest limiting connection attempts to known servers. No known exploits related to port 34571 are known as of the initial publication of this advisory, but good security practices suggest closing all unutilized ports.

DHCP Issue

If no local DHCP server exists or no static entry is made for a local DHCP server, the Cisco Unity Server will repeatedly send packets requesting an address from the DHCP server on the manufacturer's test network. Once the DHCP server address has been resolved locally, the Cisco Unity Server registry key will be updated with the DHCP server IP address and host name, and no further impact is expected.

Software Versions and Fixes

=====

The vulnerabilities are specific to the IBM-based Unity servers and all vulnerabilities listed in this advisory can be removed with specific actions to eliminate the account or addresses, so no software is required.

Obtaining Fixed Software

=====

As the fix for this vulnerability is a default configuration change, and a workaround is available, a software upgrade is not required to address this vulnerability.

If you need assistance with the implementation of the workarounds, or have questions on the workarounds, please contact the Cisco Technical Assistance Center (TAC).

Cisco 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

See <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.

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

Workarounds

=====

Local User Account Issue

Remove the "bubba" local user account. Open Computer Management, click Start, point to Settings, and then click Control Panel. Double-click Administrative Tools, and then double-click Computer Management. Click the Local Users and Group folder. Double-click the Users folder. Right-click on the "bubba" user and select Delete. The vulnerability is not present if the user "bubba" does not exist.

Raid Manager Issue

Remove all entries in the Raid Manager program for unwanted notification servers in the RaidNLst.ser file. Go to the Start menu and select Programs. Launch the ServeRAID Manager. Go to the Actions menu, select Configure ServeRAID Agent, select Notifications. In the new window right click the row for each undesired RAID Management server and select

Delete System. Close the application. There is no need to reboot. Upon exiting the program, a new RaidNLst.ser file is created with no references to any IP addresses. Do not simply delete the file without modifying the configuration via the program, as a new RaidNLst.ser file is created which contains the reference to the manufacturer's address again. The vulnerability is not present if unwanted notification servers are not present in the RaidNLst.ser file.

Set the RAID Management service to local to turn off listening on port 34571. Go to the Start menu, point to Settings, move the cursor to Control Panel and select Services. Select ServeRAID Management Service and change the properties to Disabled. Then go to the Start menu and select Programs. Launch the ServeRAID Manager and go to the File menu tab. Select User Preferences and click on the Remote Access Settings tab. Under Startup Mode check the "Local Only" checkbox. Click OK and then at the resulting dialog box click OK again. Close the application. There is no need to reboot. The vulnerability is not present if the RAID Management service is set to local.

DHCP Issue

After initial installation, to ensure the Cisco Unity Server does not send multiple DHCP requests and properly resolves its IP Address, either assign a static IP address or local address for the DHCP server. Cisco Unity server documentation discourages using DHCP for the server, recommending Cisco Unity Servers always use static IP addresses. Multiple DHCP requests will not be sent to the manufacturer's server if the Cisco Unity server is functioning with an IP address.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

Status of This Notice: FINAL

This is a final notice. Although Cisco cannot guarantee the accuracy of all statements in this notice, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this advisory unless there is some material change in the facts. Should there be a significant change in the facts, Cisco will update this advisory.

Distribution

This notice will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20031210-unity.shtml>. In addition to worldwide web posting, a text version of this notice is

Full-Disclosure: [Full-Disclosure] Cisco Security Advisory: Unity Vulnerabilities on IBM-based Servers

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
- * first-teams@first.org (includes CERT/CC)
- * bugtraq@securityfocus.com
- * full-disclosure@lists.netsys.com
- * vulnwatch@vulnwatch.org
- * cisco@spot.colorado.edu
- * cisco-nsp@puck.nether.net
- * comp.dcom.sys.cisco
- * ntbugtraq@listserv.ntbugtraq.com
- * Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

Revision History

Revision 1.0 10-December-2003 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/warp/public/707/sec_incident_response.shtml. This includes instructions for press inquiries regarding Cisco security notices. All Cisco Security Advisories are available at <http://www.cisco.com/go/psirt>.

This notice is Copyright 2003 by Cisco Systems, Inc. This notice may be redistributed freely after the release date given at the top of the text, provided that redistributed copies are complete and unmodified, and include all date and version information.

All contents are Copyright © 1992--2003 Cisco Systems, Inc. All rights reserved.

Important Notices <<http://www.cisco.com/public/copyright.html>>

PrivacyStatement <<http://www.cisco.com/public/privacy.html>>

-----BEGIN PGP SIGNATURE-----

Version: PGP 7.0.1

Full-Disclosure: [Full-Disclosure] Cisco Security Advisory: Unity Vulnerabilities on IBM-based Servers

iQA/AwUBP9dNQnsxqM8ytrWQEQJZqwCfQWMskAuHlqvT8YIYru5bRoEi1RcAn1ZW
47Gn/jvapUonII04KJbxTMXD
=r8jy
-----END PGP SIGNATURE-----

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>