# ICS-CERT ADVISORY

## ICSA-10-147-01 – CISCO NETWORK BUILDING MEDIATOR

May 27, 2010

## OVERVIEW

Cisco has identified multiple security vulnerabilities[a] in the Cisco Network Building Mediator (NBM) products. These vulnerabilities also affect the legacy Richards-Zeta Mediator products.

The following vulnerabilities have been identified: default credentials, privilege escalation, unauthorized information interception, and unauthorized information access.

Successful exploitation of any of these vulnerabilities could result in a malicious user taking complete control over an affected device.

### AFFECTED PRODUCTS

These vulnerabilities affect the legacy Richards-Zeta Mediator 2500 product and Cisco Network Building Mediator NBM-2400 and NBM-4800 models. All Mediator Framework software releases prior to 3.1.1 are affected by all vulnerabilities listed in this advisory.

### IMPACT

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation.

### BACKGROUND

Cisco Network Building Mediator collects data from sources that include the building, IT, energy supply, and energy demand systems, which use different protocols that are otherwise unable to communicate with one another. The Cisco Network Building Mediator normalizes the data into a common data representation. This ability enables the Cisco Network Building Mediator to perform any-to-any protocol translation and to provide information to the end user in a uniform presentation.

## VULNERABILITY CHARACTERIZATION

Multiple distinct vulnerabilities are in the Cisco Network Building Mediator (NBM) products. These vulnerabilities also affect the legacy Richards-Zeta Mediator products.

a. Cisco, http://www.cisco.com/en/US/products/products_security_advisory09186a0080b2c518.shtml, website last visited May 27, 2010.

## VULNERABILITY DETAILS

### DEFAULT CREDENTIALS – OVERALL CVSS SCORE 8.3[b]

Default credentials are assigned for several predefined user accounts on the device including the administrative user account. Any user with network access to the device can log in as an administrator and take complete control over the vulnerable device.

This vulnerability can be exploited remotely with authentication and without end-user interaction. Successful exploitation of this vulnerability can result in an attacker taking complete control over the vulnerable device.

The attack vectors for exploitation are through packets using these protocols and ports:

- Secure Shell (SSH) using TCP port 22
- Hypertext Transfer Protocol (HTTP) using TCP port 80
- Hypertext Transfer Protocol Secure (HTTPS) using TCP port 443
- Extensible Markup Language Remote Procedure Call (XML-RPC) over HTTP using TCP port 81
- XML-RPC over HTTPS using TCP port 443.

This vulnerability has been assigned CVE identifier CVE-2010-0595.

### PRIVILEGE ESCALATION - OVERALL CVSS SCORE 7.4[c]

Vulnerabilities in this category enable unauthorized users to read and modify device configuration. A malicious user must authenticate as an existing user but does not need to have administrator privileges or know administrator credentials to modify device configuration. Both vulnerabilities can be exploited over either transport protocol (HTTP or HTTPS).

These vulnerabilities can be exploited remotely with authentication and without end-user interaction. Successful exploitation of these vulnerabilities can result in the attacker reading and modifying the device configuration or result in a denial of service (DoS) condition as the attacker can reload the vulnerable device. Repeated attempts that successfully exploit the vulnerability that can be used to reload the vulnerable device could result in a sustained DoS condition.

The attack vectors for exploitation are through packets using these protocols and ports:

- HTTP using TCP port 80
- HTTPS using TCP port 443

b. NIST, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C, website last visited May 27, 2010.
c. NIST, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:S/C:C/I:C/A:C/E:F/RL:OF/RC:C, website last visited May 27, 2010.

- XML-RPC over HTTP using TCP port 81
- XML-RPC over HTTPS using TCP port 443.

These vulnerabilities have been assigned CVE identifiers CVE-2010-0596 and CVE-2010-0597.

## UNAUTHORIZED INFORMATION INTERCEPTION- OVERALL CVSS SCORE 7.7[d]

These vulnerabilities reflect the fact that sessions between an operator workstation and the Cisco Network Building Mediator are not protected against unauthorized interception. A malicious user able to intercept the sessions could learn any credentials used during intercepted sessions (for administrators and non-administrators alike) and could subsequently take full control of the device.

These vulnerabilities can be exploited remotely without authentication and without end-user interaction. Successful exploitation of these vulnerabilities allows information disclosure, which enables an attacker to learn information about the affected device.

The attack vectors for exploitation are through packets using these protocols and ports:

- HTTP using TCP port 80
- XML-RPC over HTTP using TCP port 81

These vulnerabilities have been assigned CVE identifiers CVE-2010-0598 and CVE-2010-0599.

## UNAUTHORIZED INFORMATION ACCESS – OVERALL CVSS SCORE 8.3[e]

A malicious user could read one of the system configuration files. This configuration file contains user accounts details, including passwords. Authentication is not required to read this configuration file, and an attacker could perform this attack over either XML RPC or XML RPC over HTTPS protocol.

This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability allows information disclosure, which enables an attacker to learn information about the affected device.

The attack vectors for exploitation are through packets using these protocols and ports:

- XML-RPC over HTTP using TCP port 81
- XML-RPC over HTTPS using TCP port 443.

This vulnerability has been assigned CVE identifier CVE-2010-0600.

Additional information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory available at http://www.cisco.com/warp/public/707/cisco-sa-20100526-mediator.shtml.

d. NIST, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C, website last visited May 27, 2010.
e. NIST, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C, website last visited May 27, 2010.

## MITIGATION

Cisco has provided information on vulnerability workarounds; they have also released free software updates that address these vulnerabilities[f].

### WORKAROUNDS

#### DEFAULT CREDENTIALS

Administrator's credentials can be changed using the procedure as described in Cisco Network Building Mediator User Guide[g]. Details of the procedure are given in section 2-10, Recovering the Cisco Network Building Mediator Password.

#### PRIVILEGE ESCALATION

There are no workarounds for these vulnerabilities.

#### UNAUTHORIZED INFORMATION INTERCEPTION

The following workaround is applicable only to the vulnerability related to HTTP protocol. There is no workaround for the vulnerability that affects XML RPC service.

The workaround for this vulnerability is to disable HTTP service and use HTTPS instead. The HTTPS service is enabled and running by default and no further actions are needed to enable it. The HTTP service can be disabled with configTOOL. The configTOOL is the software running on the operator workstation and is used to configure the Multi-Protocol Exchange of the Cisco Network Building Mediator.

After applying this workaround to software releases 1.5.1 and 2.2, configTOOL version 3.1.0b1 is required to continue configuring Cisco Network Building Mediator via configTOOL.

To start configTOOL, double-click the Cisco Network Building Mediator configTOOL shortcut icon on the desktop, or choose Start > All Programs > Network Building Mediator configTOOL. Connect to a Cisco Network Building Mediator using the procedure as described in Cisco Network Building Mediator User Guide[h] at, section 3-2 Connecting to the Cisco Network Building Mediator Using configTOOL. Inside the Node tree pane, expand the services tab, and then expand tab the network tab. Click the http_server tab, and then click the Enabled to uncheck it.

f. Cisco, http://www.cisco.com/warp/public/707/cisco-sa-20100526-mediator.shtml, website last visited May 27, 2010.
g. Cisco, http://www.cisco.com/en/US/docs/security/physical_security/cnbm/3.x/User/Guide/Mediator_User_Guide.pdf, website last visited May 27, 2010.
h. Cisco, http://www.cisco.com/en/US/docs/security/physical_security/cnbm/3.x/User/Guide/Mediator_User_Guide.pdf, website last visited May 27, 2010.

## UNAUTHORIZED INFORMATION ACCESS

There is no workaround for this vulnerability.

## LIMITING ACCESS USING IP TABLES

The following protection measure can reduce risk from unauthorized access to the Cisco Network Building Mediator and minimize the risks associated with the vulnerabilities described in this advisory. This mitigation is not effective against unauthorized information interception vulnerabilities as exploitation of these vulnerabilities do not depend on accessing the device itself, but on intercepting session between an operator console and the Cisco Network Building Mediator.

Administrators are advised to be selective when choosing the devices that are allowed to establish connections to the Cisco Network Building Mediator. The following rules will allow only legitimate operator console(s) to establish sessions to the Cisco Network Building Mediator.

```
# The following rule establishes a default policy for INPUT rule chain.
# The default policy is to drop all packets unless they are explicitly
# permitted by a rule in the INPUT chain
iptables -P INPUT DROP

# This rule will allow all traffic from operator console with
# IP address of 192.0.2.1 to the Cisco NBM
#
# Change 192.0.2.1 to match IP address used by your operators console.
iptables -I INPUT 1 --source 192.0.2.1 -j ACCEPT
```

**NOTE: When applying rules from the above example, care must be taken to allow access to ports or protocols that are used by sensors and other devices deployed in the system that are monitored and controlled by the Cisco Network Building Mediator. Failure to do so will break connectivity to these sensors and devices.**

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory.[j]

## OBTAINING UPDATED SOFTWARE

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.

i. Cisco, http://www.cisco.com/en/US/docs/security/physical_security/cnbm/3.x/User/Guide/Mediator_User_Guide.pdf, website last visited May 27, 2010.

j. Cisco, http://www.cisco.com/warp/public/707/cisco-amb-20100526-mediator.shtml, website last visited May 27, 2010.

## 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

Customers should have their product serial number available and be prepared to give the URL of the Cisco Advisory[k] as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

# REPORTING

Organizations that detect suspicious activity related to this advisory are encouraged to report to ICS-CERT for follow-on mitigation recommendations as well as tracking and correlation. Where appropriate,

k. Cisco, http://www.cisco.com/en/US/products/products_security_advisory09186a0080b2c518.shtml, website last visited May 27, 2010.

ICS-CERT is able to provide additional analytical capabilities to include onsite incident response and recovery of systems.

Organizations should follow their established internal procedures for responding to suspected incidents. Proper impact analysis and risk assessment should be performed prior to taking defensive measures.

## CONTACT ICS-CERT:

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For Control System Security Program Information and Incident Reporting:
www.ics-cert.org