Cisco Security Advisory: Cisco Router Web Setup Ships with Insecure Default IOS Configuration

Document ID: 70650

Advisory ID: cisco−sa−20060712−crws

http://www.cisco.com/warp/public/707/cisco−sa−20060712−crws.shtml

Revision 1.1

Last Updated 2006 August 10 1400 UTC (GMT)

For Public Release 2006 July 12 1600 UTC (GMT)

Please provide your feedback on this document.

Summary

The default Cisco IOS configuration shipped with the Cisco Router Web Setup (CRWS) application allows the execution of commands at privilege level 15 through the Cisco IOS HTTP (Hypertext Transfer Protocol) server web interface without requiring authentication credentials. Privilege level 15 is the highest privilege level on Cisco IOS® devices.

Fixed versions of the CRWS application have been modified by Cisco to provide a more secure default IOS configuration and additional functionality with regards to the Cisco IOS HTTP server web interface.

This issue does not require a Cisco IOS software upgrade or a CRWS software upgrade. Customers who decide to upgrade to a fixed version of CRWS and deploy the new default IOS configuration will not need to deploy the suggested workarounds. Customers who elect NOT to upgrade to a fixed CRWS version, or customers upgrading to a fixed CRWS version who keep their existing configuration should implement the workarounds identified in this advisory.

Additional information on the new default IOS configuration shipped with the CRWS application is available in the Details section of this advisory.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco−sa−20060712−crws.shtml.

Affected Products

Vulnerable Products

The following Cisco routers whose configurations have been based on the default IOS configuration shipped with any version of CRWS prior to version 3.3.0 build 31 may be affected by this vulnerability:

- Cisco 806
- Cisco 826
- Cisco 827
- Cisco 827H
- Cisco 827−4v
- Cisco 828
- Cisco 831
- Cisco 836
- Cisco 837
- Cisco SOHO 71
- Cisco SOHO 76
- Cisco SOHO 77
- Cisco SOHO 77H
- Cisco SOHO 78
- Cisco SOHO 91
- Cisco SOHO 96
- Cisco SOHO 97

Products Confirmed Not Vulnerable

Any of the previously listed Cisco routers whose IOS configuration is **not** based on the default IOS configuration shipped with the CRWS application are not vulnerable.

No other Cisco products are currently known to be affected by this vulnerability.

Details

The Cisco Router Web Setup tool (CRWS) provides a graphical user interface (GUI) for configuring Cisco SOHO and Cisco 800 series routers, and allows users to set up their routers quickly and easily. The GUI is accessed through the Cisco IOS HTTP server, which is enabled on the default IOS configuration shipped with the CRWS application.

The Cisco IOS HTTP server uses the **enable password** (assuming one has been configured) as its default authentication mechanism. Other authentication mechanisms can be configured, including the use of a local user database, an external RADIUS (Remote Authentication Dial In User Service) or an external TACACS+ (Terminal Access Controller Access Control System) server. The default IOS configuration shipped with the CRWS application does not include an **enable password** or an **enable secret** command, allowing access to the Cisco IOS HTTP server interface at any privilege level, up to and including privilege level 15, without providing authentication credentials. Privilege level 15 is the highest privilege level on Cisco IOS devices.

To resolve this vulnerability, Cisco has made changes to the default IOS configuration shipped with the CRWS application and to the CRWS application itself. Those changes are as follows:

- The addition of a default username and password combination to be used during initial device configuration.

  Note: CRWS will prompt the user to change those default credentials during its first invocation. It is strongly recommended for customers to remove those default credentials from the device configuration by using the Cisco IOS CLI (command line interface) if not planning to use the CRWS application for device configuration.
- The addition of an authentication mechanism for the Cisco IOS HTTP server to authenticate users based on the local user database.

- The addition of an access restriction to only allow connections to the Cisco IOS HTTP server from the internal network, using the addressing scheme from the default IOS configuration shipped with CRWS.

- The addition of a login banner, displayed on connections to the device through Telnet or the console port, reminding users to remove the default credentials.

- The addition of an authentication mechanism to the console port to authenticate users based on the local user database.

- A modification to the CRWS application to force users to change the default credentials the first time they access the CRWS GUI.

- A modification to the CRWS application to allow users to enable or disable access to the IOS HTTP server interface from the public interface.

This vulnerability is documented by the following Cisco bug ID:

- CSCsa78190 (registered customers only)

Note: Implementation of the available workarounds require manual configuration to mitigate the impact of this vulnerability for existing CRWS customers, even if upgrading to a fixed version of software.

Devices using CRWS for configuration and management are affected by this vulnerability if the following conditions are met:

- The current device configuration is based on the default IOS configuration shipped with the CRWS application, and

- the Cisco IOS HTTP server, which is enabled in the default IOS configuration shipped with CRWS, has not been disabled by the user, and

- no additional authentication mechanism (for example, local user database, RADIUS, TACACS+) has been defined for access to the IOS HTTP server, or no **enable password** or **enable secret** is present in the configuration.

The following procedure can be used to determine if a given device is vulnerable:

1. Is the Cisco IOS HTTP server enabled on the device?

- **YES** Proceed to step 2.

- **NO** The device is not vulnerable.

2. Is there an authentication mechanism configured for access to the IOS HTTP server interface?

- **YES** The device is not vulnerable.
- **NO** Proceed to step 3.

3. Is there an **enable password** or an **enable secret** configured on the device?

- **YES** The device is not vulnerable.
- **NO** The device is vulnerable. Please read the Software Versions and Fixes section and the Workarounds sections of this security advisory.

The following step−by−step procedure can be used in order to obtain the information needed to answer the questions in the previous procedure:

1. In order to determine if the Cisco IOS HTTP server is enabled on the device, execute the following command from a privileged CLI prompt:

   ```
   show running−config | include ip http
   ```

   The following example shows a device on which the Cisco IOS HTTP server is enabled:

   ```
   Router#show running−config | include ip http
   ip http server
   Router#
   ```

   The following example shows a device on which the Cisco IOS HTTP server is disabled:

   ```
   Router#show running−config | include ip http
   no ip http server
   Router#
   ```

   Note: Newer versions of the Cisco IOS HTTP server provide SSL (Secure Sockets Layer) encryption. This vulnerability can also be exploited if the SSL−enabled Cisco IOS HTTP server is enabled on the configuration. The following example shows a device on which the standard Cisco IOS HTTP server is disabled, but the SSL−enabled Cisco IOS HTTP server is enabled:

   ```
   Router#show running−config | include ip http
   no ip http server
   ip http secure−server
   Router#
   ```

2. In order to determine if an authentication mechanism has been applied to the Cisco IOS HTTP server, execute the following command from a privileged CLI prompt:

   ```
   show running−config | include ip http
   ```

   The following example shows a device on which the Cisco IOS HTTP server is enabled and the **local** authentication mechanism has been configured:

   ```
   Router#show running−config | include ip http
   ip http server
   ip http authentication local
   no ip http secure−server
   Router#
   ```

The absence of an **ip http authentication** line on the device configuration implies that the Cisco IOS HTTP server will use the **enable secret** or **enable password** (if so configured) as the authentication mechanism. Additional information on AAA mechanisms available for the Cisco IOS HTTP server can be found in the document entitled "AAA Control of the IOS HTTP Server", available at http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008069bdc5.shtml.

3. In order to determine if an **enable password** or **enable secret** has been configured, execute the following command from a privileged CLI prompt:

```
show running-config | include enable [secret|password]
```

The following example shows a device on which an **enable secret** password has been configured:

```
Router#show running-config | include enable [secret|password]
enable secret 5 $1$1yfp$qM7qAChXVXYp8ee2qm2Kf/
Router#
```

The following example shows a device on which no **enable password** or **enable secret** has been configured:

```
Router#show running-config | include enable [secret|password]
Router#
```

Impact

Successful exploitation of this vulnerability may allow for the execution of commands on the device at any privilege level, up to and including privilege level 15. Accessing the device at privilege level 15 would enable total control of the device, including but not limited to device configuration changes and device reloading.

Software Version and Fixes

When considering software upgrades, also consult http://www.cisco.com/go/psirt and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

This issue is fixed for new installations in CRWS version 3.3.0 build 31, which is available at http://www.cisco.com/cgi-bin/tablebuild.pl/crws.

Devices shipped from Cisco manufacturing on or after August 8, 2006, include the fixed CRWS version 3.3.0 build 31.

Information about how to install CRWS version 3.3.0 build 31 can be found at http://www.cisco.com/en/US/products/sw/netmgtsw/ps2076/prod_troubleshooting_guide09186a0080132c3c.html#108

Existing CRWS users or customers upgrading to CRWS version 3.3.0 build 31 from any previous version should deploy the workarounds mentioned in the Workarounds section of this security advisory. Upgrading the CRWS software on the device from a previous version to a fixed software version will not eliminate the vulnerability for existing installations.

Workarounds

There are multiple workarounds to mitigate this vulnerability. Existing CRWS customers, and customers upgrading to a new CRWS version from a previous one, should deploy one of the following workarounds if vulnerable to this issue. Upgrading to a new CRWS version is not enough to eliminate this vulnerability.

- **Workaround 1 Disabling the Cisco IOS HTTP Server Functionality**

  Customers not using the CRWS application to configure or manage their devices and not needing the functionality provided by the Cisco IOS HTTP server can disable it by adding the following commands to their device configuration:

  ```
  no ip http server
  no ip http secure-server
  ```

  The second command might return an error message if the Cisco IOS version installed and running on the device does not support the SSL functionality. This error message is harmless and can be safely ignored.

- **Workaround 2 Enabling Authentication of Requests to the Cisco IOS HTTP Server by Configuring an Enable Password**

  Customers using the CRWS application to configure or manage their devices, or requiring the functionality provided by the Cisco IOS HTTP server must configure an authentication mechanism for access to the Cisco IOS HTTP server interface. One of those options is to configure an **enable secret** or **enable password** password. The **enable password** is the default authentication mechanism used by the Cisco IOS HTTP server if no other method has been configured.

  In order to configure an **enable secret** password, add the following command to the device configuration:

  ```
  enable secret <mypassword>
  ```

  Replace <mypassword> with a strong password of your choosing. For guidance on strong passwords, please refer to your site security policy. The document entitled "Cisco IOS Password Encryption Facts", available at http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00801d7efa.shtml, explains the differences between the **enable secret** and the **enable password** commands.

- **Workaround 3 Enabling Authentication of Requests to the Cisco IOS HTTP Server by using an Authentication Mechanism Other than the Default**

  Configure an authentication mechanism for access to the Cisco IOS HTTP server other than the default. Such authentication mechanisms can be the local user database, or a previously defined AAA (Authentication, Authorization and Accounting) method. As the procedure to enable an authentication mechanism for the Cisco IOS HTTP server varies across Cisco IOS releases and other additional factors, no example will be provided. Customers looking for information about how to configure an authentication mechanism for the Cisco IOS HTTP server are encouraged to read the document entitled "AAA Control of the IOS HTTP Server", available at http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008069bdc5.shtml.

  Note: The only authentication method tested and supported for use with the CRWS application is the

local user database. No other methods (including the use of an external RADIUS or TACACS+ server) are supported.

In addition to those workarounds, it is highly recommended that customers limit access to their Cisco IOS HTTP server to only trusted management workstations. Information on how to restrict access to the Cisco IOS HTTP server based on IP addresses can be found at http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca734.h

Obtaining Fixed Software

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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 is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was discovered during internal testing.

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 advisory is posted on Cisco's worldwide website at http://www.cisco.com/warp/public/707/cisco−sa−20060712−crws.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
- first−teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco−nsp@puck.nether.net
- full−disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

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 1.1	2006 August 10 1400 UTC	Added information on new devices including the fixed

	(GMT)	CRWS release.
Revision 1.0	2006 July 12 1600 UTC (GMT)	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.

Updated: Aug 10, 2006 Document ID: 70650