

Cisco Security Response: Potential Exploitation of Default Administrative Credentials

<http://www.cisco.com/warp/public/707/cisco-sr-20070215-http.shtml>

Revision 1.0

For Public Release 2007 Feb 15 1600 UTC (GMT)

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

Contents

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

Cisco Response

This is a response to a Symantec published research paper posted on their website at http://www.symantec.com/enterprise/security_response/weblog/2007/02/driveby_pharming_how_clickin and http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf, and entitled 'Drive-by Pharming'. In particular, this response focuses on the information in the Symantec paper, as relevant to certain of Cisco's non-consumer products. These products are specified in the '[Cisco Routers Impacted](#)' section below.

Purpose of this Response

As the paper does not disclose any new vulnerability in Cisco products, Cisco is issuing this response and not a Security Advisory. The purpose of this response is to inform customers how to change any default credentials which may ship pre-configured on an impacted Cisco router (identified below), upon initial configuration and before the device is connected to a public network.

Cisco Routers Impacted

Several types of Cisco routers that are marketed for the Small Office/Home Office (SOHO), Remote

Office/Branch Office (ROBO) and Teleworker business segments may include either Cisco Router Web Setup tool (CRWS) or Cisco Router and Security Device Manager (SDM), which are web-based device-management tools for Cisco IOS® Software-based routers.

Those Cisco routers have the Cisco IOS HTTP server enabled by default, to allow CRWS or SDM to communicate with the router. With either CRWS or SDM installed at shipping, the routers configuration will have a default username and password that is used to access the router via the HTTP web interface.

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 attack methodology if the default username and password have not been removed:

- 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

The following Cisco routers, whose configurations have been based on the default IOS configuration shipped with any version of SDM prior to version 2.3.3, may be affected by this attack methodology if the default username and password have not been removed.

For details regarding which units have SDM default configurations enabled at shipping, please consult Table 4: "Ordering and Factory Shipping Options for Cisco SDM" at:
http://www.cisco.com/en/US/prod/collateral/routers/ps5318/product_data_sheet0900aecd800fd118.html

Cisco SDM-Supported Routers	Cisco SDM-Supported Cisco IOS Releases
Cisco SB101	
Cisco SB106	12.3(8)YG, 12.4(2)T or later releases
Cisco SB107	
	12.2(13)ZH or later releases
Cisco 831	12.3(2)XA or later releases

Cisco 837	12.3(2)T or later releases 12.4(2)T or later releases
Cisco 836	12.2(13)ZH or later releases 12.3(2)XA or later releases 12.3(4)T or later releases 12.4(2)T or later releases
Cisco 851	12.3(8)YI
Cisco 857	12.4(2)T or later releases
Cisco 871	12.3(8)YI 12.4(2)T or later releases
Cisco 876	
Cisco 877	
Cisco 878	
Cisco 1701	12.2(13)ZH or later releases 12.3(2)XA or later releases (Cisco SDM does not support Cisco IOS release 12.3(2)XF.) 12.3(4)T or later releases 12.4(2)T or later releases
Cisco 1711	12.2(15)ZL or later releases 12.3(2)XA or later releases
Cisco 1712	(Cisco SDM does not support Cisco IOS release 12.3(2)XF.) 12.4(2)T or later releases
Cisco 1710	12.2(13)ZH or later releases 12.3(2)XA or later releases
Cisco 1721	(Cisco SDM does not support Cisco IOS release 12.3(2)XF.)

Cisco 1751	12.2(13)T3 or later releases
Cisco 1751-v	12.3(2)T or later releases
Cisco 1760	12.3(1)M or later releases
Cisco 1760-v	12.2(15)ZJ3 (not available for the Cisco 1710 or Cisco 1721) 12.4(2)T or later releases
Cisco 1801	
Cisco 1802	12.3(8)YI
Cisco 1803	12.4(2)T or later releases
Cisco 1811	
Cisco 1812	12.3(8)YH or later releases 12.4(2)T or later releases
Cisco 1841	12.3(8)T4 or later releases 12.4(2)T or later releases
Cisco 2610XM	12.2(11)T6 or later releases
Cisco 2611XM	12.3(2)T or later releases
Cisco 2620XM	12.3(1)M or later releases
Cisco 2621XM	12.3(4)XD
Cisco 2650XM	12.2(15)ZJ3
Cisco 2651XM	12.4(2)T or later releases
Cisco 2691	
Cisco 2801	
Cisco 2811	12.3(8)T4 or later releases
Cisco 2821	12.4(2)T or later releases
Cisco 2851	
	12.2(11)T6 or later releases
	12.2(11)T6 or later releases

	12.3(2)T or later releases
Cisco 3640	12.3(1)M or later releases
Cisco 3661	12.3(4)XD
Cisco 3662	12.2(15)ZJ3
	12.4(2)T or later releases
Cisco 3620	12.2(11)T6 or later releases
	12.3(1)M or later releases
Cisco 3640A	12.2(13)T3 or later releases
	12.3(2)T or later releases
	12.3(1)M or later releases
	12.3(4)XD
	12.2(15)ZJ3
	12.4(2)T or later releases
Cisco 3725	12.2(11)T6 or later releases
	12.3(2)T or later releases
Cisco 3745	12.3(1)M or later releases
	12.3(4)XD
	12.2(15)ZJ3
	12.4(2)T or later releases
Cisco 3825	12.3(11)T or later releases
Cisco 3845	12.4(2)T or later releases
Cisco 7204VXR	12.3(2)T or later releases
	12.3(1)M or later releases
Cisco 7206VXR	12.4(2)T or later releases
	Cisco SDM does not support B, E, or S train releases on the Cisco 7000 routers.

Cisco 7301	12.3(2)T or later releases
	12.3(3)M or later releases
	12.4(2)T or later releases
	Cisco SDM does not support B, E, or S train releases on the Cisco 7000 routers.

Any of the previously listed Cisco routers whose IOS configuration is not based on the default IOS configuration shipped with either the CRWS or SDM application are not affected by this attack methodology.

Additional Information

The Cisco IOS HTTP server is enabled by default on several Cisco IOS devices for use with web-based configuration tools such as CRWS or SDM. If those products are configured via either CRWS or SDM, administrators will be prompted to change the default administrative credentials when they try to configure the device for the first time (earlier versions of CRWS did NOT request the changing of default credentials. For details see <http://www.cisco.com/warp/public/707/cisco-sa-20060712-crws.shtml>).

If the device first-time configuration is done using the command line interface (CLI) and not through the web-based interface, the administrator will NOT be prompted to change the default credentials nor will they be removed automatically by the device itself. Not changing or removing the default credentials leaves the device open to potential exploitation, as described in Symantec's research paper.

Cisco introduced a new security feature via Cisco Bug ID [CSCse65910](#) ([registered](#) customers only) , per which Cisco IOS has added a new keyword 'one-time' to the usernames. User credentials configured on the device and using the 'one-time' option can only be used once when the user connects to the router through a virtual terminal (vty) line or Console port. Cisco IOS will remove this credential from the running configuration after the initial use. The administrator of the device, should then add a username with a privilege level of 15 using the following command:

```
username "myuser" privilege 15 secret 0 "mypassword"
```

Replace 'myuser' and 'mypassword' with the username and password you choose to use, and save the changes to the startup configuration.

SDM takes advantage of this Cisco IOS feature from SDM version 2.3.3 or later. This feature is documented on Cisco Bug Toolkit as Cisco Bug ID [CSCek35024](#) ([registered](#) customers only) .

Cisco encourages customers to change any default credentials being used by those device managers during first use.

Recommended Workarounds

To help mitigate the risks associated with the type of attack presented in the Symantec paper, Cisco

recommends that any default credentials shipped with the device (username/password combinations) be completely removed. If the Cisco router is not configured nor monitored by either SDM or CRWS, and if the IOS HTTP server is not required in your environment, it should be disabled.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this response:

<http://www.cisco.com/warp/public/707/cisco-amb-20070215-http.shtml>

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

Customers who do not use the CRWS or SDM device-management tools and not requiring 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 who use the CRWS or SDM device-management tools, or requiring the functionality provided by the Cisco IOS HTTP server should configure an authentication mechanism for access to the Cisco IOS HTTP server interface. One option is to configure an enable secret or enable password. The enable password is the default authentication mechanism used by the Cisco IOS HTTP server if no other method has been configured.

To configure authentication of the http access via the enable secret password, add the following commands to the device configuration:

```
enable secret "mypassword"
ip http authentication enable
```

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_note09186a00809d38a7.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**

Instead of configuring authentication using the default method as described in Workaround 2, configure an authentication mechanism for access to the Cisco IOS HTTP server via other mechanisms. 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.

References

- Definition of Pharming
The definition of pharming from "[Protect Against Social Engineering](#)" is shown below:
" Pharming also takes advantage of false websites, by redirecting users to the false site as they attempt to access a legitimate website. This redirection, also known as domain spoofing, can be perpetrated through an e-mailed virus that lies dormant on a PC until the user enters a specific URL, or by poisoning a domain name system (DNS) directory. A DNS translates web and e-mail addresses into numeric strings. In a poisoned DNS, the links that associate web addresses with numeric strings are changed so users are directed to a false website when they enter a specific URL. Any secure information entered into the false website, such as a user name and password, is captured by hackers. "
- Improving Security on Cisco Routers
The document "[Improving Security on Cisco Routers](#)" is an informal discussion of some Cisco configuration settings that network administrators should consider changing on their routers, especially on their border routers, in order to improve security.

Revision History

Revision 1.0	2007-Feb-15	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>.

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)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)