

Cisco Applied Mitigation Bulletin: Prevention of the Exploitation of the Default Web Interface Administrative Credentials

Document ID: 82004

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

Revision 1.0

For Public Release 2007 February 15 1600 UTC (GMT)

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

[Cisco Response](#)
[User Education and Security Awareness Training](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)
[Related Information](#)

Cisco Response

Vulnerability Characteristics

The Exploitation of the Default Web Interface Administrative Credentials can be accomplished locally by using the default credentials shipped with some products. A user must visit a malicious website for this attack to be successful. If this is exploited, the attacker may change the network device configuration, may create a denial of service (DoS) condition or may gain complete control of the device. The attack vector is through TCP port 80. This vulnerability is not covered by a CVE ID.

This document contains information to assist Cisco customers in mitigating attempts to Exploit the Default Web Interface Administrative Credentials. Potentially vulnerable devices include Cisco SOHO routers, including the 800 series. Additional information is available in the PSIRT Security Response: <http://www.cisco.com/warp/public/707/cisco-sr-20070215-http.shtml>.

Mitigation Technique Overview

The most preventive form of protection a home network administrator can take against these types of attacks is changing the default device password during the setup process. Many device types mentioned in the Symantec advisory ship with a default password or a blank password. Many devices in these categories also ship with software to aid in the device setup process. During the device setup process, the default or blank password should be changed to a non default password using strong password creation techniques. These techniques include the use of mixed-case letters, numbers, and punctuation symbols. For additional information on choosing a secure password, refer to the US-CERT Cyber Security Tip ST04-002 Choosing and Protecting Passwords, available at: <http://www.us-cert.gov/cas/tips/ST04-002.html>. During the use of the software setup programs supplied with these devices, the home network administrator is asked to change the default device password. If this step is completed, this will prevent the successful Exploitation of the Default Web Interface Administrative Credentials.

User Education and Security Awareness Training

To reduce the risk that users will fall victim to Exploitation of the Default Web Interface Administrative Credentials, it is advisable to educate them about safe browsing. Countermeasures should also be implemented at the application level (the browser) through the scripting controls available in the browser. Scripting controls allow the definition of policy to restrict code execution. A standard strategy should consist of the following:

- Disable all scripting languages interpreted by the browser.



Caution: Disabling scripting may result in a loss of functionality because many web applications use scripting. Take care to ensure that all required business applications are fully functional with scripting disabled.

- Only follow links to known websites from trusted sources.
- Enable URL verification (phishing detection) in the browser if available.



- Caution:** Enabling URL verification may leak information to external networks.
- Disregard unsolicited e-mail messages containing URLs.

The effectiveness of any mitigation technique 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 is the most appropriate for use in the intended network before it is deployed.

Additional Information

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.

Revision History

Revision 1.0	2007 February 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>.

Related Information

- **Improving Security on Cisco Routers:**
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
-

