

# Cisco Security Advisory: 7xx Router Password Buffer Overflow

Document ID: 13666

Advisory ID: cisco-sa-19971216-pw-buffer

<http://www.cisco.com/warp/public/707/cisco-sa-19971216-pw-buffer.shtml>

## Revision 2.0

Last Updated 1998 June 16 1500 UTC (GMT)

For Public Release 1997 December 16 0100 UTC (GMT)

---

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

---

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of This Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

---

## Summary

Some Cisco 7xx routers can be crashed by connecting with TELNET and typing very long password strings. There exists a small possibility that this bug could be exploited to launch other attacks against the router, other than simply crashing it.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19971216-pw-buffer.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

All Cisco 7xx routers running IOS/700 software version 4.1(1), 4.1(2), or 4.1 interim releases earlier than 4.1(2.1) are affected. Systems running releases earlier than 4.1 are *not* affected. In order to exploit the vulnerability, an attacker must have access to the password prompt. This means that the attacker must be able to TELNET to the target router, or to gain access to its console port.

This vulnerability affects systems running IOS/700 version 4.1 releases, including 4.1(1), 4.1(2), and 4.1 interim releases earlier than 4.1(2.1). IOS/700 releases other than 4.1 are *not* affected. 4.2 and later releases are not affected.

## Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

## Details

This vulnerability has been assigned bug ID CSCdj66458.

[View CSCdj66458](#)

Insufficient bounds checking on the data buffer used for password input allows the incoming password to exceed the buffer size, overwriting the contents of memory beyond the end of the buffer. When the system tries to use the now-incorrect data in that memory, unpredictable results occur. If the data are randomly chosen, this unpredictable behavior can be expected to result in the detection of errors, such as accesses to illegal addresses, which result in system crashes. It might be possible to craft a data string that, instead of creating detectable errors, causes particular system behavior desired by the attacker. However, Cisco development engineers have been unable to construct such a string.

## Impact

This vulnerability allows attackers to force 7xx routers to reboot, denying service to legitimate users during the reboot period, and possibly causing excessive "call flapping" as routers shut down and restart.

It is possible that including the right data at the right place in the too-long password string could enable an attacker to take complete control of the router, or to cause it to hang indefinitely. Engineering analysis of the data structures surrounding the affected buffer has not revealed any viable way of doing this. A person who succeeds in such an attack would be able to reconfigure the router or modify its functionality, theoretically in any way at all.

## Software Versions and Fixes

A software fix was integrated in IOS/700 version 4.1(2.1). The first regular production release containing this fix was 4.2(1). Cisco will be making the fixed software available to all IOS/700 customers who are presently running 4.1 software, regardless of contract status. Customers under contract may obtain the software through their regular upgrade channels. Customers not under contract should contact the Cisco TAC and reference the URL of this document.

## Workarounds

The vulnerability may be avoided by controlling access to the system console port, and by restricting access to the TELNET facility to trusted hosts.

TELNET access may be restricted either by using filters on firewalls or surrounding routers, or by using filters on the 7xx router itself. To restrict access to the TELNET service on a 7xx router running 4.1(x) software to a single trusted management host, use the command

```
set ip filter tcp in source = not trusted-ip-address destination = 7xx-address:23 block
```

The command should be applied in every profile that may be active when the router is connected to a potentially hostile network.

## Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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](mailto: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

Cisco has had no known reports of malicious exploitation of this vulnerability.

This vulnerability has been discussed on the "bugtraq@netspace.org" mailing list, and is therefore certain to be widely known in the cracker community. The first public announcement of this vulnerability of which Cisco is aware was on December 11, 1997.

The vulnerability can be exploited to crash systems with no special tools or knowledge; no exploitation program as such is required.

Assuming that it is possible to exploit the vulnerability to take total control of the system, an exploitation program would be needed in order to do so. A person seeking to develop such an exploitation program would need to be a competent assembly language programmer. She would also need detailed knowledge of the internal workings of the IOS/700 software and/or the 7xx router hardware. Such knowledge has not been made public by Cisco, but could be obtained by reverse engineering or by theft of trade secrets from Cisco.

## 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

The initial interim version of this notice was sent to the following Internet mailing lists and newsgroups:

- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)

Future versions of this notice will be posted on Cisco's Web site, but will not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the Web site for updates.

This notice will be posted in the "[Field Notices](#)" section of Cisco's Worldwide Web site, which can be found under "Technical Tips" in the "Software and Support" section. The URL is <http://www.cisco.com/warp/public/707/cisco-sa-19971216-pw-buffer.shtml>. The copy on the Worldwide Web will be updated as appropriate.

## Revision History

Revision 2.0	<del>1998-June-16</del>	Updated to reflect software
	1997-December-16	fix availability. Initial version.

## Cisco Security Procedures

Please report security issues with Cisco products, and/or sensitive security intrusion emergencies involving Cisco products, to [security-alert@cisco.com](mailto:security-alert@cisco.com). Reports may be encrypted using PGP; public RSA and DSS keys for security-alert@cisco.com are on the public PGP key servers.

The alias [security-alert@cisco.com](mailto:security-alert@cisco.com) is used only for reports incoming to Cisco. Mail sent to security-alert@cisco.com goes only to a very small group of users within Cisco. Neither outside users nor unauthorized Cisco employees may subscribe to security-alert@cisco.com.

Please do not use security-alert@cisco.com for configuration questions, for security intrusions that you do not consider to be sensitive emergencies, or for general, non-security-related support requests. We do not have the capacity to handle such requests through this channel, and will have to refer them to [Cisco's Technical Assistance Center](#), delaying response to your questions. We advise contacting the Technical Assistance Center directly with this type of question. TAC contact numbers 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](mailto:tac@cisco.com)

All formal public security notices generated by Cisco are sent to the public mailing list: "cust-security-announce@cisco.com". For information on subscribing to this mailing list, send a message containing the single line "info cust-security-announce" to "majordomo@cisco.com". "cust-security-discuss@cisco.com" is an analogous list available for public discussion of the notices and other Cisco security issues.

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

---

Updated: Jun 16, 1998

Document ID: 13666

---