

Cisco Security Advisory: Cisco 7600 Series Router Session Border Controller Denial of Service Vulnerability

Advisory ID: cisco-sa-20090304-sbc

<http://www.cisco.com/warp/public/707/cisco-sa-20090304-sbc.shtml>

Revision 1.0

For Public Release 2009 March 4 1600 UTC (GMT)

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

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring 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

A denial of service (DoS) vulnerability exists in the Cisco Session Border Controller (SBC) for the Cisco 7600 series routers. Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090304-sbc.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

All Cisco ACE-based SBC modules running software versions prior to 3.0(2) are affected.

To determine the version of the Cisco SBC software running on a system, log in to the device and issue the **show version** command to display the system banner.

```
card_A/Admin# show version
  system image file: [LCP] disk0:c76-sbck9-
mzg.3.0.1_AS3_0_00.bin
<output truncated>
```

Cisco SBC software version 3.0.1 is running in the device used in this example.

☐ Products Confirmed Not Vulnerable

The Cisco XR 12000 Series SBC is not vulnerable. Additionally, the Cisco ACE Module, Cisco ACE 4710 Application Control Engine, Cisco ACE XML Gateway, Cisco ACE Web Application Firewall, and the Cisco ACE GSS (Global Site Selector) 4400 Series are not affected by this vulnerability. No other Cisco products are currently known to be affected by this vulnerability.

[Top of the section](#) [Close Section](#)

☐ Details

The Session Border Controller (SBC) enables direct IP-to-IP interconnect between multiple administrative domains for session-based services providing protocol interworking, security, and admission control and management. The SBC is a multimedia device that sits on the border of a network and controls call admission to that network. A vulnerability exists in the Cisco SBC where an unauthenticated attacker may cause the Cisco SBC card to reload by sending crafted TCP packets over port 2000. Repeated exploitation could result in a sustained DoS condition.

Note: Only the Cisco SBC module reloads after successful exploitation. The Cisco 7600 series router does not reload and it is not affected by this vulnerability.

Note: TCP port 2000 is typically used by Skinny Call Control Protocol (SCCP) applications. However, the Cisco SBC module uses TCP port 2000 for high availability (redundancy) communication, but does not use the SCCP for this purpose.

This vulnerability is documented in Cisco Bug IDs [CSCsq18958](#) ([registered](#) customers only) ; and has been assigned the Common Vulnerability and Exposures (CVE) IDs CVE-2009-0619.

[Top of the section](#) [Close Section](#)

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

CSCsq18958 - Crafted TCP packet may crash SBC					
Calculate the environmental score of CSCsq18958					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#) [Close Section](#)

[-] Impact

Successful exploitation of the vulnerability may cause a reload of the affected device. Repeated exploitation could result in a sustained DoS condition.

[Top of the section](#) [Close Section](#)

[-] Software Versions and Fixes

This vulnerability has been corrected in Cisco SBC software release 3.0(2).

Cisco SBC software can be downloaded from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/sbc-7600-crypto>

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.

[Top of the section](#) [Close Section](#)

☐ Workarounds

As a workaround, configure an access control list (ACL) in the signaling / media VLAN on the Route Processor (RP). The following examples show how VLAN 140 is configured as the signaling / media VLAN. A separate VLAN (VLAN 77) is configured as Fault Tolerance (FT). An ACL is added to the signaling/media VLAN on the RP filtering all TCP port 2000 packets to the alias IP address.

Cisco SBC configuration

```
interface vlan 140
  ip address 10.140.1.90 255.255.255.0
  alias 10.140.1.100 255.255.255.0
  peer ip address 10.140.1.8 255.255.255.0
!
ft interface vlan 77
  ip address 192.168.1.1 255.255.255.0
  peer ip address 192.168.1.8 255.255.255.0
```

RP Configuration

```
!- ACL blocking all TCP port 2000 traffic to the
10.140.1.0 internal network
!
access-list 100 deny    tcp any host 10.140.1.100 eq 2000
access-list 100 permit ip any any
!
interface Vlan140
  ip address 10.140.1.1 255.255.255.0
!- ACL is applied to the VLAN interface to egress traffic
  ip access-group 100 out
!
```

The alias command under VLAN 140 is configured with an IP address that floats between active and standby modules when using high availability. Only TCP port 2000 traffic destined to this IP

address may trigger this vulnerability. An access control list (ACL) is configured to deny TCP port 2000 destined to the alias IP address (10.140.1.100). The ACL is applied egress in the RP.

Note: TCP port 2000 is used by Skinny Call Control Protocol (SCCP) applications; however, in this case it is used by the SBC for internal communications. The previous ACL only blocks TCP port 2000 traffic to the alias IP address. TCP port 2000 is not used by the alias IP address. This ACL should not cause any collateral damage.

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

<http://www.cisco.com/warp/public/707/cisco-amb-20090304-sbc.shtml>

[Top of the section](#) [Close Section](#)

☐ **Obtaining Fixed Software**

Cisco has released free software updates that address this vulnerability. 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/en/US/docs/general/warranty/English/EU1KEN.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact 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 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 this notice 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.

[Top of the section](#) [Close Section](#)

☐ **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 found during internal testing.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20090304-sbc.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-bulletins@lists.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.

[Top of the section](#) [Close Section](#)

☐ **Revision History**

Revision 1.0	2009-March-04	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](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)