

Cisco Security Response: Catalyst 6500 and Cisco 7600 Series Devices Accessible via Loopback Address

<http://www.cisco.com/warp/public/707/cisco-sr-20070926-lb.shtml>

Revision 1.2

Last Updated 2008 February 20 1600 UTC (GMT)

For Public Release 2007 September 26 2200 UTC (GMT)

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

Contents

[Cisco Response](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

Cisco Response

This document is the Cisco PSIRT response to an issue regarding Cisco Catalyst 6500 and Cisco 7600 series devices that was discovered and reported to Cisco by Lee E. Rian.

The original report has been posted to full-disclosure mailing list.

Cisco PSIRT greatly appreciates the opportunity to work with researchers on security vulnerabilities, and we welcome the opportunity to review and assist in product reports.

This vulnerability is documented in Cisco bug ID [CSCek49649](#) ([registered](#) customers only)

This Cisco Security Response is available at the following link: <http://www.cisco.com/warp/public/707/cisco-sr-20070926-lb.shtml>

Additional Information

Cisco Catalyst 6500 and Cisco 7600 series devices use addresses from the 127.0.0.0/8 (loopback) range in the Ethernet Out-of-Band Channel (EOBC) for internal communication.

Addresses from this range that are used in the EOBC on Cisco Catalyst 6500 and Cisco 7600 series devices are accessible from outside of the system. The Supervisor module, Multilayer Switch Feature Card (MSFC), or any other intelligent module may receive and process packets that are destined for the 127.0.0.0/8 network. An attacker can exploit this behavior to bypass existing access control lists that do not filter 127.0.0.0/8 address range; however, an exploit will not allow an attacker to bypass authentication or authorization. Valid authentication credentials are still required to access the modules that require authentication and are configured for it.

Per RFC 3330, a packet that is sent to an address anywhere within the 127.0.0.0/8 address range should loop back inside the host and should never reach the physical network. However, some host implementations send packets to addresses in the 127.0.0.0/8 range outside their Network Interface Card (NIC) and to the network. Certain implementations that normally do not send packets to addresses in the 127.0.0.0/8 range may also be configured to do so.

Destination addresses in the 127.0.0.0/8 range are not routed on the Internet. This factor limits the exposure of this issue.

This issue is applicable to systems that run Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the MSFC) and Native Mode (IOS Software on both the Supervisor Engine and the MSFC).

This issue has been documented by the Cisco bug ID [CSCek49649](#) ([registered](#) customers only) . All software versions that run on Cisco Catalyst 6500 and Cisco 7600 series devices are affected. A fix is available in 12.2(33)SXH.

As a workaround, administrators can apply an access control list that filters packets to the 127.0.0.0/8 address range to interfaces where attacks may be launched.

```
ip access-list extended block_loopback
  deny ip any 127.0.0.0 0.255.255.255
  permit ip any any

interface Vlan x
  ip access-group block_loopback in
```

Control Plane Policing (CoPP) can be used to block traffic with a destination IP address in the 127.0.0.0/8 address range sent to the device. Cisco IOS Software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks. CoPP protects the management and control planes by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations.

```
!-- Permit all traffic with a destination IP
!-- addresses in the 127.0.0.0/8 address range sent to
!-- the affected device so that it will be policed and
!-- dropped by the CoPP feature
!

access-list 111 permit icmp any 127.0.0.0 0.255.255.255
access-list 111 permit udp any 127.0.0.0 0.255.255.255
access-list 111 permit tcp any 127.0.0.0 0.255.255.255
access-list 111 permit ip any 127.0.0.0 0.255.255.255

!
!-- Permit (Police or Drop)/Deny (Allow) all other Layer3
!-- and Layer4 traffic in accordance with existing security
!-- policies and configurations for traffic that is
authorized
!-- to be sent to infrastructure devices
!
!-- Create a Class-Map for traffic to be policed by the
!-- CoPP feature
!

class-map match-all drop-127/8-netblock-class
  match access-group 111

!
!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.
!
```

```
policy-map drop-127/8-netblock-traffic
  class drop-127/8-netblock-class
    police 32000 1500 1500 conform-action drop exceed-
action drop

!
!-- Apply the Policy-Map to the Control-Plane of the
!-- device
!

control-plane
  service-policy input drop-127/8-netblock-traffic

!
```

Additional information on the configuration and use of the CoPP feature is available at the following links:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.html

Infrastructure Access Control Lists (iACLs) are also considered a network security best practice and should be considered as, long-term additions to effective network security as well as a workaround for this specific issue. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs. The white paper is available at the following link:

<http://www.cisco.com/warp/public/707/iacl.html>

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-20070926-lb.shtml>

Additional Information

Revision History

| | | |
|--------------|-------------------|--|
| Revision 1.2 | 2008-Feb-20 | Changed the bug ID to CSCek49649. Fixed software stays the same. |
| Revision 1.1 | 2007-September-28 | Revised Additional Information section. |
| Revision 1.0 | 2007-September-26 | 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>.

| | | | | | | |
|----------------------|----------------------------|-----------------------|-------------------------|--------------------------|--------------------------|----------------------|
| 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.](#)