Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco 7600 Series Router Session Border Controller Denial of Service Vulnerability

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

Revision 1.0

For Public Release 2009 March 04 1600 UTC (GMT)

Please provide your feedback on this document.

Contents

Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory *Cisco 7600 Series Router Session Border Controller Denial of Service Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

The Cisco Session Border Controller (SBC) for Cisco 7600 Series routers contains a vulnerability that may result in a Denial of Service (DoS) condition. This DoS condition may occur when the Cisco SBC processes malformed TCP packets that are sent on port 2000. This vulnerability can be exploited remotely without authentication and without end-user interaction. The attack vector for exploitation is through malformed packets using TCP port 2000.

This vulnerability has been assigned CVE identifier CVE-2009-0619.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory, which is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090304-sbc.shtml

Mitigation Technique Overview

Cisco devices provide several countermeasures for this vulnerability. Administrators are advised to consider these protection methods to be general security best practices for infrastructure devices and the traffic that transits the network. This section of the document provides an overview of these techniques.

Cisco IOS Software can provide effective means of exploit prevention using infrastructure access control lists (iACLs). This protection mechanism filters and drops packets that are attempting to exploit this vulnerability.

Effective exploit prevention can also be provided by the Cisco ASA 5500 Series Adaptive Security Appliance, the Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers using transit access control lists (tACLs).

These protection mechanisms filter and drop packets that are attempting to exploit this vulnerability.

Cisco IOS NetFlow flow records can provide visibility into network-based exploitation attempts.

Cisco IOS Software, Cisco ASA appliances, Cisco PIX security appliances, and FWSM firewalls can provide visibility through syslog messages and the counter values displayed in the output from **show** commands.

Risk Management

Organizations are advised to follow their standard risk evaluation and mitigation processes to determine the potential impact of this vulnerability. Triage refers to sorting projects and prioritizing efforts that are most likely to be successful. Cisco has provided documents that can help organizations develop a risk-based triage capability for their information security teams. Risk Triage for Security Vulnerability Announcements and Risk Triage and Prototyping can help organizations develop repeatable security evaluation and response processes.

Device Specific Mitigation and Identification

 **Caution:** The effectiveness of any mitigation technique depends on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. As with any configuration change, evaluate the impact of this configuration prior to applying the change.

Specific information about mitigation and identification is available for these devices:

- Cisco IOS Routers and Switches
- Cisco IOS NetFlow
- Cisco ASA, PIX, and FWSM Firewalls

Cisco IOS Routers and Switches

Mitigation: Infrastructure Access Control Lists

To protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators are advised to deploy infrastructure access control lists (iACLs) to perform policy enforcement of traffic sent to infrastructure equipment. Administrators can construct an iACL by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. For the maximum protection of infrastructure devices, deployed iACLs should be applied in the ingress direction on all interfaces to which an IP address has been configured. An iACL workaround cannot provide complete protection against this vulnerability when the attack originates from a trusted source address.

The iACL policy denies unauthorized packets on TCP port 2000 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices, and there are no trusted sources that require access to the affected devices on TCP port 2000. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of iACLs.

Additional information about iACLs is in Protecting Your Core: Infrastructure Protection Access Control Lists.

```
ip access-list extended Infrastructure-ACL-Policy


 !
 !-- The following vulnerability-specific access control entry
 !-- (ACE) can aid in identification of attacks
 !

 deny tcp any 192.168.60.0 0.0.0.255 eq 2000


 !
 !-- Explicit deny ACE for traffic sent to addresses configured within
 !-- the infrastructure address space
 !

 deny ip any 192.168.60.0 0.0.0.255


 !
 !-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
 !-- with existing security policies and configurations
 !

 !-- Apply iACL to interfaces in the ingress direction
 !

interface GigabitEthernet0/0
 ip access-group Infrastructure-ACL-Policy in
```

Note that filtering with an interface access list will elicit the transmission of ICMP unreachable

messages back to the source of the filtered traffic. Generating these messages could have the undesired effect of increasing CPU utilization on the device. In Cisco IOS Software, ICMP unreachable generation is limited to one packet every 500 milliseconds by default. ICMP unreachable message generation can be disabled using the interface configuration command **no ip unreachables**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable** *interval-in-ms*.

Identification: Infrastructure Access Control Lists

After the administrator applies the iACL to an interface, the **show ip access-lists** command will identify the number of packets on TCP port 2000 that have been filtered on interfaces on which the iACL is applied. Administrators should investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show ip access-lists Infrastructure-ACL-Policy** follows:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
    10 deny tcp any 192.168.60.0 0.0.0.255 eq 2000 (32 matches)
    20 deny ip any 192.168.60.0 0.0.0.255 (11 matches)
router#
```

In the preceding example, access list *Infrastructure-ACL-Policy* has dropped **32** packets on **TCP port 2000** for access control list entry (ACE) line 10.

For additional information about investigating incidents using ACE counters and syslog events, reference the Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence white paper.

Administrators can use Embedded Event Manager to provide instrumentation when specific conditions are met, such as ACE counter hits. The Applied Intelligence white paper Embedded Event Manager in a Security Context provides additional details about how to use this feature.

Identification: Access List Logging

The **log** and **log-input** access control list (ACL) option will cause packets that match specific ACEs to be logged. The **log-input** option enables logging of the ingress interface in addition to the packet source and destination IP addresses and ports.

 **Caution:** Access control list logging can be very CPU intensive and must be used with extreme caution. Factors that drive the CPU impact of ACL logging are log generation, log transmission, and process switching to forward packets that match log-enabled ACEs.

For Cisco IOS Software, the **ip access-list logging interval** *interval-in-ms* command can limit the effects of process switching induced by ACL logging. The **logging rate-limit** *rate-per-second* [**except** *loglevel*] command limits the impact of log generation and transmission.

The CPU impact from ACL logging can be addressed in hardware on the Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers with Supervisor Engine 720 or Supervisor Engine 32 using optimized ACL logging.

For additional information about the configuration and use of ACL logging, reference the Understanding Access Control List Logging Applied Intelligence white paper.

Cisco IOS NetFlow

Identification: Traffic Flow Identification Using NetFlow Records

Administrators can configure Cisco IOS NetFlow on Cisco IOS routers and switches to aid in the identification of traffic flows that may be attempts to exploit the vulnerability. Administrators are advised to investigate flows to determine whether they are attempts to exploit the vulnerability or whether they are legitimate traffic flows.

```
router#show ip cache flow
IP packet size distribution (90784136 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  48
   .000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .00

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  1885 active, 63651 inactive, 59960004 added
  129803821 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
  0 active, 16384 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Se
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet    11393421      2.8         1    48      3.1       0.0       1.4
TCP-FTP           236       0.0        12    66      0.0       1.8       4.8
TCP-FTPD           21       0.0     13726  1294      0.0      18.4       4.1
TCP-WWW         22282       0.0        21  1020      0.1       4.1       7.3
TCP-X             719       0.0         1    40      0.0       0.0       1.3
TCP-BGP             1       0.0         1    40      0.0       0.0      15.0
TCP-Frag        70399       0.0         1   688      0.0       0.0      22.7
TCP-other     47861004      11.8         1   211     18.9       0.0       1.3
UDP-DNS           582       0.0         4    73      0.0       3.4      15.4
UDP-NTP         287252      0.0         1    76      0.0       0.0      15.5
UDP-other       310347      0.0         2   230      0.1       0.6      15.9
ICMP             11674      0.0         3    61      0.0      19.8      15.5
IPv6INIP            15      0.0         1  1132      0.0       0.0      15.4
GRE                  4      0.0         1    48      0.0       0.0      15.3
Total:        59957957      14.8         1   196     22.5       0.0       1.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pk
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  06 0984 07D0
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  06 0911 07D0
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    06 0016 12CA
Gi0/0         192.168.13.97   Gi0/1         192.168.60.28   11 0B3E 0050
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   06 0B89 07D0
Gi0/0         10.88.226.1     Gi0/1         192.168.202.22  11 007B 007B
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  11 0BD7 00A1
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016
router#
```

In the preceding example, there are multiple flows for **TCP** port **2000 (hex value 07D0)** packets sent to the 192.168.60.0 address block.

To view only the traffic flows for packets on TCP port 2000 (hex value 07D0), the command **show ip cache flow | include SrcIf|_06_.*07D0** will display the related TCP NetFlow records as shown

here:

```
router#show ip cache flow | include SrcIf|_06_.*07D0
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pk
Gi0/0         192.168.10.201  Gi0/1         192.168.60.102  06 0984 07D0
Gi0/0         192.168.11.54   Gi0/1         192.168.60.158  06 0911 07D0
Gi0/0         192.168.10.17   Gi0/1         192.168.60.97   06 0B89 07D0
router#
```

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

To protect the network from traffic that enters the network at ingress access points, which may include Internet connection points, partner and supplier connection points, or VPN connection points, administrators are advised to deploy tACLs to perform policy enforcement. Administrators can construct a tACL by explicitly permitting only authorized traffic to enter the network at ingress access points or permitting authorized traffic to transit the network in accordance with existing security policies and configurations. A tACL workaround cannot provide complete protection against this vulnerability when the attack originates from a trusted source address.

The tACL policy denies unauthorized packets on TCP port 2000 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices, and there are no trusted hosts that require access to the affected devices on TCP port 2000. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic.

Additional information about tACLs is in Transit Access Control Lists: Filtering at Your Edge.

```
!
!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks
!


access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0 eq


!
!-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!

!-- Explicit deny for all other IP traffic
!


access-list tACL-Policy extended deny ip any any


!
!-- Apply tACL to interface(s) in the ingress direction
!

access-group tACL-Policy in interface outside
```

Identification: Transit Access Control Lists

After the tACL has been applied to an interface, administrators can use the **show access-list** command to identify the number of packets on TCP port 2000 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list tACL-Policy** follows:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 2 elements
access-list tACL-Policy line 1 extended deny tcp any 192.168.60.0 255.255.25
access-list tACL-Policy line 2 extended deny ip any any (hitcnt=8)
firewall#
```

In the preceding example, access list *tACL-Policy* has dropped **119** packets on **TCP port 2000** received from an untrusted host or network destined for affected devices. In addition, syslog message *106023* can provide valuable information, which includes the source and destination IP address, the source and destination port numbers, and the IP protocol for the denied packet.

Identification: Firewall Access List Syslog Messages

Firewall syslog message *106023* will be generated for packets denied by an access control entry (ACE) that does not have the **log** keyword present. Additional information about this syslog message is in Cisco Security Appliance System Log Message - 106023.

Information about configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500 Series Security Appliance is in Monitoring the Security Appliance - Configuring and Managing Logs. Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is in Monitoring the Firewall Services Module.

In the following example, the **show logging | grep** *regex* command extracts syslog messages from the logging buffer on the firewall. These messages provide additional information about denied packets that could indicate potential attempts to exploit the vulnerability that is described in this document. It is possible to use different regular expressions with the **grep** keyword to search for specific data in the logged messages.

Additional information about regular expression syntax is in Creating a Regular Expression.

```
firewall#show logging | grep 106023
  Feb 21 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2944
         dst inside:192.168.60.191/2000 by access-group "tACL-Policy"
  Feb 21 2009 00:15:14: %ASA-4-106023: Deny tcp src outside:192.2.0.200/2945
         dst inside:192.168.60.33/2000 by access-group "tACL-Policy"
  Feb 21 2009 00:25:34: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2946
         dst inside:192.168.60.240/2000 by access-group "tACL-Policy"
  Feb 21 2009 00:25:35: %ASA-4-106023: Deny tcp src outside:192.2.0.200/2947
         dst inside:192.168.60.115/2000 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *tACL-Policy* show packets for **TCP port 2000** sent to the address block assigned to the affected devices.

Additional information about syslog messages for ASA and PIX security appliances is in Cisco Security Appliance System Log Messages. Additional information about syslog messages for the FWSM is in Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging System Log Messages.

For additional information about investigating incidents using syslog events, reference the Identifying Incidents Using Firewall and IOS Router Syslog Events Applied Intelligence white

paper.

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	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.

Related Information

- **Cisco Applied Mitigation Bulletins**
- **Cisco Security Center**
- **Cisco IOS NetFlow - Home Page on Cisco.com**
- **Cisco IOS NetFlow White Papers**
- **NetFlow Performance Analysis**
- **Cisco Network Foundation Protection White Papers**
- **Cisco Network Foundation Protection Presentations**
- **A Security-Oriented Approach to IP Addressing**
- **Cisco Firewall Products - Home Page on Cisco.com**
- **Common Vulnerabilities and Exposures (CVE)**

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Send