

# Cisco Applied Mitigation Bulletin: Detecting and Mitigating Exploitation of Multiple OpenSSL Vulnerabilities

Document ID: 72012

<http://www.cisco.com/warp/public/707/cisco-amb-20061108-openssl.shtml>

## Revision 1.0

For Public Release 2006 November 08 1600 UTC (GMT)

---

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

---

[Cisco Response](#)  
[Device-Specific Mitigation and Identification](#)  
[Additional Information](#)  
[Revision History](#)  
[Cisco Security Procedures](#)

---

## Cisco Response

### Vulnerability Characteristics

Four OpenSSL vulnerabilities have been identified within certain Cisco products. An attacker could use these vulnerabilities to access protected resources, cause a denial of service (DoS) condition, or execute code.

- A denial of service vulnerability exists when processing invalid ASN.1 structures. This vulnerability can be exploited remotely. No authentication or user interaction is required. This vulnerability is covered by CVE ID 2006-2937.
- A denial of service vulnerability exists when processing public keys. This vulnerability can be exploited remotely. No authentication or user interaction is required. This vulnerability is covered by CVE ID 2006-2940.
- An RSA signature forgery vulnerability could allow an attacker to access signature-protected resources. This vulnerability can be exploited remotely. No authentication or user interaction is required. This vulnerability is covered by CVE ID 2006-4339.
- A buffer overflow vulnerability in the *SSL\_get\_shared\_ciphers()* function could allow an attacker to cause a DoS condition or execute code. This vulnerability can be exploited remotely. No authentication or user interaction is required. This vulnerability is covered by CVE ID 2006-3738.

This document contains information to assist Cisco customers in mitigating attempts to exploit the aforementioned OpenSSL vulnerabilities. Vulnerable, nonaffected, and fixed software information is available in the PSIRT Security Advisory at <http://www.cisco.com/warp/public/707/cisco-sr-20061108-openssl.shtml>.

### Mitigation Technique Overview

Cisco devices provide several countermeasures for Cisco products that use and are affected by these OpenSSL vulnerabilities. When available, the most preventive control is provided by preventing access to potentially vulnerable applications at the network level on the target endpoint through the use of access lists (ACLs) or

other similar functionality. Other forms of access control may not be sufficient to prevent exploitation. In cases in which the application of ACLs directly to the affected device is not feasible, Cisco firewalls and routers can provide threat mitigation from nonmanagement IP addresses through the use of transit access control lists (transit ACLs). OpenSSL is most often associated with the HTTPS protocol (TCP/443) and this is the most likely attack vector for most of the vulnerabilities. However, the most likely attack vector for the RSA signature forgery vulnerability (CVE ID 2006–4339) is the SSH protocol (TCP/22). In some cases, these protocols may be configured to use a different port that depends on the administrator's choice. It is possible that vulnerable libraries could be linked to other applications using different ports or protocols and that these protocols could potentially be used for exploitation. For the purpose of this document, the HTTPS and SSH protocols will be allowed limited access from trusted sources while all other protocols are blocked.

## Device–Specific Mitigation and Identification

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

- [Internet Edge Routers](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)
- [Cisco Switches](#)

### Internet Edge Routers



**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.

#### Mitigation

Transit ACLs can limit access to devices affected by these OpenSSL vulnerabilities. The following transit ACL is designed to permit access from trusted management stations to the HTTPS and SSH protocols and deny all other IP access to the affected device. Classification ACLs are used after the permit statements to aid in identifying attack attempts. In this example, the trusted management station IP addresses are 192.168.100.1 and 192.168.100.2, and the affected device IP address is 172.16.100.2. Added access list entries should be implemented as part of a transit ACL that filters transit and edge traffic at network ingress points. For more information on transit ACLs, refer to [Transit Access Control Lists: Filtering at Your Edge](#).

```
!--Allow HTTPS and SSH from trusted source addresses only.

access-list 150 permit tcp host 192.168.100.1 host 172.16.100.2 eq 443
access-list 150 permit tcp host 192.168.100.2 host 172.16.100.2 eq 443
access-list 150 permit tcp host 192.168.100.1 host 172.16.100.2 eq 22
access-list 150 permit tcp host 192.168.100.2 host 172.16.100.2 eq 22

!-- Block HTTPS and SSH from all other source addresses.
!-- This is useful for identifying attack attempts.

access-list 150 deny tcp any host 172.16.100.2 eq 443
access-list 150 deny tcp any host 172.16.100.2 eq 22

!-- Deny all other access to the affected device(s).

access-list 150 deny ip any host 172.16.100.2
```

```
!-- Permit/deny other traffic in accordance with existing security policy.
```

```
interface serial 2/0  
  access-group 150 in
```

## Identification

After the interface ACL is applied to the ingress interface, the command **show access-list *acl number*** can be used to identify the number of packets being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit OpenSSL vulnerabilities.

The following is an example of output for the **show access-list 150** command. In the example, 18 HTTPS and two SSH packets have been dropped by the access list configured inbound on interface Serial 2/0.

```
Edge-Router#show access-list 150  
Extended IP access list 150  
 10 permit tcp host 192.168.100.1 host 172.16.100.2 eq 443 (110 matches)  
 20 permit tcp host 192.168.100.2 host 172.16.100.2 eq 443 (110 matches)  
 30 permit tcp host 192.168.100.1 host 172.16.100.2 eq 22 (95 matches)  
 40 permit tcp host 192.168.100.2 host 172.16.100.2 eq 22 (87 matches)  
 50 deny tcp any host 172.16.100.2 eq 443 (18 matches)  
 60 deny tcp any host 172.16.100.2 eq 22 (2 matches)
```

## Cisco ASA, PIX, and FWSM Firewalls

### Mitigation: Cisco ASA and PIX 7.x

Transit ACLs can limit access to devices affected by these OpenSSL vulnerabilities. The following transit ACL is designed to permit access from trusted management stations to the HTTPS and SSH protocols and deny all other IP access to the affected device. Classification ACLs are used after the permit statements to aid in identifying attack attempts. In this example, the trusted management station IP addresses are 192.168.100.1 and 192.168.100.2, and the affected device IP address is 172.16.100.2.

```
access-list ssl remark Allow access from trusted management sources for HTTPS and SSH.  
access-list ssl extended permit tcp host 192.168.100.1 host 172.16.100.2 eq https  
access-list ssl extended permit tcp host 192.168.100.2 host 172.16.100.2 eq https  
access-list ssl extended permit tcp host 192.168.100.2 host 172.16.100.2 eq ssh  
access-list ssl extended permit tcp host 192.168.100.1 host 172.16.100.2 eq ssh
```

```
!-- Deny access from non trusted sources for HTTPS and SSH.
```

```
access-list ssl extended deny tcp any host 172.16.100.2 eq https  
access-list ssl extended deny tcp any host 172.16.100.2 eq ssh
```

```
!-- Deny all other access to the affected device(s).
```

```
access-list ssl extended deny ip any host 172.16.100.2
```

```
!-- Permit/deny other traffic in accordance with existing security policy.
```

```
access-group ssl in interface outside
```

### Identification: Cisco ASA and PIX 7.x

The following is an example of output for the **show access-list *ssl*** command. In the example, 22 HTTPS and 10 SSH packets have been dropped by the access list configured inbound on interface outside. These packets may be an attempt to exploit OpenSSL vulnerabilities and should be investigated.

```
R4-ASA5520a#show access-list ssl
```

```

access-list ssl; 7 elements
access-list ssl line 1 Allow access from trusted management sources for HTTPS and SSH
access-list ssl line 2 extended permit tcp host 192.168.100.1
  host 172.16.100.2 eq https (hitcnt=209)
access-list ssl line 3 extended permit tcp host 192.168.100.2
  host 172.16.100.2 eq https (hitcnt=209)
access-list ssl line 4 extended permit tcp host 192.168.100.2
  host 172.16.100.2 eq ssh (hitcnt=44)
access-list ssl line 5 extended permit tcp host 192.168.100.1
  host 172.16.100.2 eq ssh (hitcnt=10)
access-list ssl line 6 extended deny tcp any host 172.16.100.2
  eq https (hitcnt=22)
access-list ssl line 7 extended deny tcp any host 172.16.100.2
  eq ssh (hitcnt=10)
access-list ssl line 8 extended deny ip any host 172.16.100.2 (hitcnt=33)

```

## Mitigation: Firewall Services Module

Transit ACLs can limit access to devices affected by these OpenSSL vulnerabilities. The following transit ACL is designed to permit access from trusted management stations to the HTTPS and SSH protocols and deny all other IP access to the affected device. Classification ACLs are used after the permit statements to aid in identifying attack attempts. In this example, the trusted management station IP addresses are 192.168.100.1 and 192.168.100.2, and the affected device IP address is 172.16.100.2.

```

!-- Allow access from trusted management sources for HTTPS and SSH.

access-list ssl extended permit tcp host 192.168.100.1 host 172.16.100.2 eq https
access-list ssl extended permit tcp host 192.168.100.2 host 172.16.100.2 eq https
access-list ssl extended permit tcp host 192.168.100.2 host 172.16.100.2 eq ssh
access-list ssl extended permit tcp host 192.168.100.1 host 172.16.100.2 eq ssh

!-- Deny access from all other sources for HTTPS and SSH.

access-list ssl extended deny tcp any host 172.16.100.2 eq https
access-list ssl extended deny tcp any host 172.16.100.2 eq ssh

!-- Deny all other access to the affected device(s).

access-list ssl extended deny ip any host 172.16.100.2

!-- Permit/deny other traffic in accordance with existing security policy.

access-group ssl in interface outside

```

## Identification: Firewall Services Module

The following is an example of output for the **show access-list ssl** command. In the example, 22 HTTPS and 10 SSH packets have been dropped by the access list configured inbound on interface outside. These packets may be an attempt to exploit OpenSSL vulnerabilities and should be investigated.

```

FWSM#show access-list ssl
access-list ssl; 7 elements
access-list ssl line 1 Allow access from trusted management sources for HTTPS and SSH
access-list ssl line 2 extended permit tcp host 192.168.100.1
  host 172.16.100.2 eq https (hitcnt=291)
access-list ssl line 3 extended permit tcp host 192.168.100.2
  host 172.16.100.2 eq https (hitcnt=290)
access-list ssl line 4 extended permit tcp host 192.168.100.2
  host 172.16.100.2 eq ssh (hitcnt=53)
access-list ssl line 5 extended permit tcp host 192.168.100.1
  host 172.16.100.2 eq ssh (hitcnt=14)
access-list ssl line 6 extended deny tcp any host 172.16.100.2

```

```
    eq https (hitcnt=22)
access-list ssl line 7 extended deny tcp any host 172.16.100.2
    eq ssh (hitcnt=10)
access-list ssl line 8 extended deny ip any host 172.16.100.2 (hitcnt=0)
```

## Cisco Switches



**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.

### Mitigation

Transit ACLs can limit access to devices affected by these OpenSSL vulnerabilities. The following transit ACL is designed to permit access from trusted management stations to the HTTPS and SSH protocols and deny all other IP access to the affected device. Classification ACLs are used after the permit statements to aid in identifying attack attempts. In this example, the trusted management station IP addresses are 192.168.100.1 and 192.168.100.2, and the affected device IP address is 172.16.100.2.

```
!--Allow HTTPS and SSH from trusted source addresses only.

access-list 150 permit tcp host 192.168.100.1 host 172.16.100.2 eq 443
access-list 150 permit tcp host 192.168.100.2 host 172.16.100.2 eq 443
access-list 150 permit tcp host 192.168.100.1 host 172.16.100.2 eq 22
access-list 150 permit tcp host 192.168.100.2 host 172.16.100.2 eq 22

!-- Block HTTPS and SSH from all other source addresses.
!-- This is useful for identifying attack attempts.

access-list 150 deny tcp any host 172.16.100.2 eq 443
access-list 150 deny tcp any host 172.16.100.2 eq 22

!-- Deny all other access to the affected device(s).

access-list 150 deny ip any host 172.16.100.2

!-- Permit/deny other traffic in accordance with existing security policy.

interface VLAN2
    access-group 150 out
```

### Identification

After the interface ACL is applied to the ingress interface, the command **show access-list *acl number*** can be used to identify the number of packets being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit OpenSSL vulnerabilities.

The following is an example of output for the **show access-list** command. In the example, 18 HTTPS and two SSH packets have been dropped by the access list configured outbound on interface VLAN2. These packets may be an attempt to exploit OpenSSL vulnerabilities and should be investigated.

```
R4-Cat6509Ea#show access-list 150
Extended IP access list 150
 10 permit tcp host 192.168.100.1 host 172.16.100.2 eq 443 (110 matches)
 20 permit tcp host 192.168.100.2 host 172.16.100.2 eq 443 (110 matches)
 30 permit tcp host 192.168.100.1 host 172.16.100.2 eq 22 (19 matches)
 40 permit tcp host 192.168.100.2 host 172.16.100.2 eq 22 (21 matches)
```

```
50 deny tcp any host 172.16.100.2 eq 443 (18 matches)
60 deny tcp any host 172.16.100.2 eq 22 (2 matches)
70 deny ip any host 172.16.100.2 (9 matches)
```

## 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	2006–November–08	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](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>.

---

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

---

Updated: Nov 08, 2006

Document ID: 72012

---