

# Cisco Security Advisory: Multiple Vulnerabilities in Cisco ASA Adaptive Security Appliance and Cisco PIX Security Appliances

Advisory ID: cisco-sa-20090408-asa

<http://www.cisco.com/warp/public/707/cisco-sa-20090408-asa.shtml>

## Revision 1.2

Last Updated 2009 April 13 1800 UTC (GMT)

For Public Release 2009 April 08 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

Multiple vulnerabilities exist in the Cisco ASA 5500 Series Adaptive Security Appliances and Cisco PIX Security Appliances. This security advisory outlines the details of these vulnerabilities:

- VPN Authentication Bypass when Account Override Feature is Used vulnerability
- Crafted HTTP packet denial of service (DoS) vulnerability
- Crafted TCP Packet DoS vulnerability
- Crafted H.323 packet DoS vulnerability
- SQL\*Net packet DoS vulnerability
- Access control list (ACL) bypass vulnerability

Workarounds are available for some of the vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090408-asa.shtml>.

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

## ☐ **Affected Products**

### ☐ **Vulnerable Products**

The following is a list of the products affected by each vulnerability as described in detail within this advisory.

#### **VPN Authentication Bypass Vulnerability**

Cisco ASA or Cisco PIX security appliances that are configured for IPsec or SSL-based remote access VPN and have the Override Account Disabled feature enabled are affected by this vulnerability.

**Note:** The Override Account Disabled feature was introduced in Cisco ASA software version 7.1(1). Cisco ASA and PIX software versions 7.1, 7.2, 8.0, and 8.1 are affected by this vulnerability. This feature is disabled by default.

#### **Crafted HTTP Packet DoS Vulnerability**

Cisco ASA security appliances may experience a device reload that can be triggered by a series of crafted HTTP packets, when configured for SSL VPNs or when configured to accept Cisco Adaptive Security Device Manager (ASDM) connections. Only Cisco ASA software versions 8.0 and 8.1 are affected by this vulnerability.

#### **Crafted TCP Packet DoS Vulnerability**

Cisco ASA and Cisco PIX security appliances may experience a memory leak that can be triggered by a series of crafted TCP packets. Cisco ASA and Cisco PIX security appliances running versions 7.0, 7.1, 7.2, 8.0, and 8.1 are affected when configured for any of the following features:

- SSL VPNs
- ASDM Administrative Access
- Telnet Access
- SSH Access
- Cisco Tunneling Control Protocol (cTCP) for Remote Access VPNs
- Virtual Telnet
- Virtual HTTP
- Transport Layer Security (TLS) Proxy for Encrypted Voice Inspection
- Cut-Through Proxy for Network Access
- TCP Intercept

## **Crafted H.323 Packet DoS Vulnerability**

Cisco ASA and Cisco PIX security appliances may experience a device reload that can be triggered by a series of crafted H.323 packets, when H.323 inspection is enabled. H.323 inspection is enabled by default. Cisco ASA and Cisco PIX software versions 7.0, 7.1, 7.2, 8.0, and 8.1 are affected by this vulnerability.

## **SQL\*Net Packet DoS Vulnerability**

Cisco ASA and Cisco PIX security appliances may experience a device reload that can be triggered by a series of SQL\*Net packets, when SQL\*Net inspection is enabled. SQL\*Net inspection is enabled by default. Cisco ASA and Cisco PIX software versions 7.2, 8.0, and 8.1 are affected by this vulnerability.

## **Access Control List Bypass Vulnerability**

A vulnerability exists in the Cisco ASA and Cisco PIX security appliances that may allow traffic to bypass the implicit deny behavior at the end of ACLs that are configured within the device. Cisco ASA and Cisco PIX software versions 7.0, 7.1, 7.2, and 8.0 are affected by this vulnerability.

## **Determination of Software Versions**

The show version command-line interface (CLI) command can be used to determine whether a vulnerable version of the Cisco PIX or Cisco ASA software is running. The following example shows a Cisco ASA Adaptive Security Appliance that runs software version 8.0(4):

```
ASA#show version

Cisco Adaptive Security Appliance Software Version 8.0(4)
Device Manager Version 6.0(1)

<output truncated>
```

The following example shows a Cisco PIX security appliance that runs software version 8.0(4):

```
PIX#show version

Cisco PIX Security Appliance Software Version 8.0(4)
Device Manager Version 5.2(3)
```

<output truncated>

Customers who use Cisco ASDM to manage their devices can find the software version displayed in the table in the login window or in the upper left corner of the ASDM window.

## ☐ **Products Confirmed Not Vulnerable**

The Cisco Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers and Cisco VPN 3000 Series Concentrators are not affected by any of these vulnerabilities. Cisco PIX Security Appliance Software versions 6.x are not affected by any of these vulnerabilities. No other Cisco products are currently known to be affected by these vulnerabilities.

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

## ☐ **Details**

This Security Advisory describes multiple distinct vulnerabilities. These vulnerabilities are independent of each other.

### **VPN Authentication Bypass Vulnerability**

The Cisco ASA or Cisco PIX security appliance can be configured to override an account-disabled indication from a AAA server and allow the user to log on anyway. However, the user must provide the correct credentials in order to login to the VPN. A vulnerability exists in the Cisco ASA and Cisco PIX security appliances where VPN users can bypass authentication when the override account feature is enabled.

**Note:** The override account feature was introduced in Cisco ASA software version 7.1(1).

The override account feature is enabled with the **override-account-disable** command in **tunnel-group general-attributes** configuration mode, as shown in the following example. The following example allows overriding the "account-disabled" indicator from the AAA server for the WebVPN tunnel group "testgroup":

```
hostname(config)#tunnel-group testgroup type webvpn  
hostname(config)#tunnel-group testgroup general-attributes  
hostname(config-tunnel-general)#override-account-disable
```

**Note:** The override account feature is disabled by default.

This vulnerability is documented in Cisco Bug ID [CSCsx47543](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) identifiers CVE-2009-1155.

### **Crafted HTTP Packet DoS Vulnerability**

A crafted SSL or HTTP packet may cause a DoS condition on a Cisco ASA device that is configured to terminate SSL VPN connections. This vulnerability can also be triggered to any interface where ASDM access is enabled. A successful attack may result in a reload of the device. A TCP three-way

handshake is needed to exploit this vulnerability.

This vulnerability is documented in Cisco Bug ID [CSCsv52239](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) identifiers CVE-2009-1156.

### **Crafted TCP Packet DoS Vulnerability**

A crafted TCP packet may cause a memory leak on a Cisco ASA or Cisco PIX device. A successful attack may result in a sustained DoS condition. A Cisco ASA device configured for any of the following features is affected:

- SSL VPNs
- ASDM Administrative Access
- Telnet Access
- SSH Access
- cTCP for Remote Access VPNs
- Virtual Telnet
- Virtual HTTP
- TLS Proxy for Encrypted Voice Inspection
- Cut-Through Proxy for Network Access
- TCP Intercept

**Note:** This vulnerability may be triggered when crafted packets are sent to any TCP based service that terminates on the affected device. The vulnerability may also be triggered via transient traffic only if the TCP intercept features has been enabled. A TCP three-way handshake is not needed to exploit this vulnerability.

This vulnerability is documented in Cisco Bug ID [CSCsy22484](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) identifiers CVE-2009-1157.

### **Crafted H.323 Packet DoS Vulnerability**

A crafted H.323 packet may cause a DoS condition on a Cisco ASA device that is configured with H.323 inspection. H.323 inspection is enabled by default. A successful attack may result in a reload of the device. A TCP three-way handshake is not needed to exploit this vulnerability.

This vulnerability is documented in Cisco Bug ID [CSCsx32675](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) identifiers CVE-2009-1158.

### **SQL\*Net Packet DoS Vulnerability**

The SQL\*Net protocol consists of different packet types are handled by the security appliance to make the data stream appear consistent to the Oracle version 7.x and earlier implementations on either side of the Cisco ASA and Cisco PIX security appliances. A series of SQL\*Net packets may cause a denial of service condition on a Cisco ASA and Cisco PIX device that is configured with SQL\*Net inspection. SQL\*Net inspection is enabled by default. A successful attack may result in a reload of the device.

The default port assignment for SQL\*Net is TCP port 1521. This is the value used by Oracle for SQL\*Net. Please note the **class-map** command can be used in the Cisco ASA or Cisco PIX to apply

SQL\*Net inspection to a range of different port numbers. A TCP three-way handshake is needed to exploit this vulnerability. The requirement of a TCP three way handshake significantly reduces the possibility of exploitation using packets with spoofed source addresses.

This vulnerability is documented in Cisco Bug ID [CSCsw51809](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) identifiers CVE-2009-1159.

## Access Control List Bypass Vulnerability

Access lists have an implicit deny behavior that is applied to packets that have not matched any of the permit or deny ACEs in an ACL and reach the end of the ACL. This implicit deny is there by design, does not require any configuration and can be understood as an implicit ACE that denies all traffic reaching the end of the ACL. A vulnerability exists in the Cisco ASA and Cisco PIX that may allow traffic to bypass the implicit deny ACE.

**Note:** This behavior only impacts the implicit deny statement on any ACL applied on the device. Access control lists with explicit deny statements are not affected by this vulnerability. This vulnerability is experienced in very rare occasions and extremely hard to reproduce.

You can trace the lifespan of a packet through the security appliance to see whether the packet is operating correctly with the packet tracer tool. The **packet-tracer** command provides detailed information about the packets and how they are processed by the security appliance. If a command from the configuration did not cause the packet to drop, the **packet-tracer** command will provide information about the cause in an easily readable manner. You can use this feature to see if the implicit deny on an ACL is not taking effect. The following example shows that the implicit deny is bypassed (result = ALLOW):

```
<output truncated>
...
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
  Forward Flow based lookup yields rule:
    in  id=0x1a09d350, priority=1, domain=permit, deny=false
        hits=1144595557, user_data=0x0, cs_id=0x0, l3_type=0x8
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0000.0000.0000

<output truncated>
```

This vulnerability is documented in Cisco Bug ID [CSCsq91277](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) identifiers CVE-2009-1160.

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

## ▣ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities 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>.

<b>CSCsx47543 - AAA account-override-ignore allows VPN session without correct password</b>					
<b>Calculate the environmental score of <a href="#">CSCsx47543</a></b>					
CVSS Base Score - <b>7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	None	None
CVSS Temporal Score - <b>6.8</b>					
Exploitability		Remediation Level		Report Confidence	
High		Official-Fix		Confirmed	

<b>CSCsv52239 - Cisco ASA may crash with certain HTTP packets</b>					
<b>Calculate the environmental score of <a href="#">CSCsv52239</a></b>					
CVSS Base Score - <b>7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - <b>6.4</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

<b>CSCsy22484 - Cisco ASA may crash after processing certain TCP</b>					
--	--	--	--	--	--

**packets**

**Calculate the environmental score of [CSCsy22484](#)**

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

**CSCsx32675- Crafted H.323 packet may cause ASA to reload**

**Calculate the environmental score of [CSCsx32675](#)**

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

**CSCsw51809 - sqlnet traffic causes traceback with inspection configured**

**Calculate the environmental score of [CSCsw51809](#)**

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 - **6.8**

Exploitability	Remediation Level	Report Confidence
High	Official-Fix	Confirmed

**CSCsq91277 - ACL Misbehavior in Cisco ASA**

**Calculate the environmental score of [CSCsq91277](#)**

CVSS Base Score - **4.3**

Access	Access		Confidentiality	Integrity	Availability
--------	--------	--	-----------------	-----------	--------------

Vector	Complexity	Authentication	Impact	Impact	Impact
Network	Medium	None	Partial	None	None
CVSS Temporal Score - <b>3.6</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

## ▣ Impact

Successful exploitation of the VPN Authentication Bypass when Account Override Feature is Used vulnerability may allow an attacker to successfully connect to the Cisco ASA via remote access IPsec or SSL-based VPN. The Denial of Service (DoS) vulnerabilities may cause a reload of the affected device. Repeated exploitation could result in a sustained DoS condition. Successful exploitation of the ACL bypass vulnerability may allow an attacker to access resources that should be protected by the Cisco ASA.

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

## ▣ Software Versions and Fixes

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.

The following table contains the first fixed software release of each vulnerability. The "Recommended Release" row indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. A device running a version of the given release in a specific row (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Release" row of the table.

Vulnerability	Affected Release	First Fixed Version	Recommended Release
VPN Authentication Bypass when Account Override Feature is Used	7.0	Not vulnerable	7.0(8)6
	7.1	7.1(2)82	7.1(2)82
	7.2	7.2(4)27	7.2(4)30
	8.0	8.0(4)25	8.0(4)28

Vulnerability	8.1	8.1(2)15	8.1(2)19
Crafted HTTP packet DoS Vulnerability	7.0	Not vulnerable	7.0(8)6
	7.1	Not vulnerable	7.1(2)82
	7.2	Not vulnerable	7.2(4)30
	8.0	8.0(4)25	8.0(4)28
	8.1	8.1(2)15	8.1(2)19
Crafted TCP Packet DoS Vulnerability	7.0	7.0(8)6	7.0(8)6
	7.1	7.1(2)82	7.1(2)82
	7.2	7.2(4)30	7.2(4)30
	8.0	8.0(4)28	8.0(4)28
	8.1	8.1(2)19	8.1(2)19
Crafted H.323 packet DoS Vulnerability	7.0	7.0(8)6	7.0(8)6
	7.1	7.1(2)82	7.1(2)82
	7.2	7.2(4)26	7.2(4)30
	8.0	8.0(4)24	8.0(4)28
	8.1	8.1(2)14	8.1(2)19
Crafted SQL packet DoS vulnerability	7.0	Not vulnerable	7.0(8)6
	7.1	Not vulnerable	7.1(2)82
	7.2	7.2(4)26	7.2(4)30
	8.0	8.0(4)22	8.0(4)28
	8.1	8.1(2)12	8.1(2)19
Access control list (ACL) bypass vulnerability	7.0	7.0(8)1	7.0(8)6
	7.1	7.1(2)74	7.1(2)82
	7.2	7.2(4)9	7.2(4)30
	8.0	8.0(4)5	8.0(4)28
	8.1	Not vulnerable	8.1(2)19

Fixed Cisco ASA software can be downloaded from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ASAPSIRT>

Fixed Cisco PIX software can be downloaded from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/PIXPSIRT>

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

## ☐ Workarounds

This Security Advisory describes multiple distinct vulnerabilities. These vulnerabilities and their respective workarounds are independent of each other.

### VPN Authentication Bypass Vulnerability

The override account feature is enabled with the **override-account-disable** command in **tunnel-group general-attributes** configuration mode. As a workaround, disable this feature using the **no override-account-disable** command.

### Crafted HTTP Packet DoS Vulnerability

Devices configured for SSL VPN (clientless or client-based) or accepting ASDM management connections are vulnerable.

**Note:** IPSec clients are not vulnerable to this vulnerability.

If SSL VPN (clientless or client-based) is not used, administrators should make sure that ASDM connections are only allowed from trusted hosts.

To identify the IP addresses from which the security appliance accepts HTTPS connections for ASDM, configure the **http** command for each trusted host address or subnet. The following example, shows how a trusted host with IP address 192.168.1.100 is added to the configuration:

```
hostname(config)# http 192.168.1.100 255.255.255.255
```

### Crafted TCP Packet DoS Vulnerability

There are no workarounds for this vulnerability.

### Crafted H.323 Packet DoS Vulnerability

H.323 inspection should be disabled if it is not needed. Temporarily disabling the feature will mitigate this vulnerability. H.323 inspection can be disabled with the command **no inspect h323**.

### SQL\*Net Packet DoS Vulnerability

SQL\*Net inspection should be disabled if it is not needed. Temporarily disabling the feature will mitigate this vulnerability. SQL\*Net inspection can be disabled with the command **no inspect sqlnet**.

## Access Control List (ACL) Bypass Vulnerability

As a workaround, remove the **access-group** line applied on the interface where the ACL is configured and re-apply it. For example:

```
ASA(config)#no access-group acl-inside in interface inside
ASA(config)#access-group acl-inside in interface inside
```

In the previous example the access group called **acl-inside** is removed and reapplied to the inside interface. Alternatively, you can add an explicit **deny ip any any** line in the bottom of the ACL applied on that interface. For example:

```
ASA(config)#access-list 100 deny ip any any
```

In the previous example, an explicit deny for all IP traffic is added at the end of **access-list 100**.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory, which is available at the following link: <http://www.cisco.com/warp/public/707/cisco-amb-20090408-asa.shtml>.

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

## ☐ Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. 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](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](mailto: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](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 aware of a publicly available proof of concept exploit for the crafted TCP packet DoS vulnerability. The Cisco PSIRT is not aware of any public announcements or malicious use of the other vulnerabilities described in this advisory.

The crafted TCP packet DoS vulnerability was discovered and reported to Cisco by Gregory W. MacPherson and Robert J. Combo from Verizon Business.

The ACL bypass vulnerability was reported to Cisco by Jon Ramsey, Jeff Jarmoc, and Fernando Medrano from SecureWorks.

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

All other vulnerabilities were found during internal testing and during the resolution of customer service requests.

[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-20090408-asa.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](mailto:cust-security-announce@cisco.com)
- [first-bulletins@lists.first.org](mailto:first-bulletins@lists.first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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 1.2	2009-April-13	Changed recommended release from 8.1(2)16 to 8.1(2)19 in Crafted HTTP packet DoS Vulnerability section of software table.
Revision 1.1	2009-April-08	<a href="#">Exploitation and Public Announcements</a> update.
Revision	2009-	

1.0	April-08	Initial public release.
-----	----------	-------------------------

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

## ☐ 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/docs/general/warranty/English/EU1KEN\\_.html](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

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

---

### 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)

☐