

[VulnWatch] Cisco Security Advisory: Multiple IOS IPS Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-02/msg00010.html>

- *From:* Cisco Systems Product Security Incident Response Team <psirt@xxxxxxxx>
 - *Date:* Tue, 13 Feb 2007 11:50:46 -0500
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Cisco Security Advisory: Multiple IOS IPS Vulnerabilities

Advisory ID: cisco-sa-20070213-iosips

<http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.shtml>

Revision 1.0

For Public Release 2007 February 13 1600 UTC (GMT)

Summary

=====

The Intrusion Prevention System (IPS) feature set of Cisco IOS contains several vulnerabilities. These include:

- * Fragmented IP packets may be used to evade signature inspection.
- * IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.shtml>.

Affected Products

=====

Vulnerable Products

+-----

The following Cisco IOS release trains with the IPS feature set enabled are vulnerable to the fragmented packet evasion vulnerability:

- * 12.3T, except versions 12.3(2)T, 12.3(4)T, and 12.3(7)T
- * 12.4
- * 12.4T
- * 12.4XE

The following Cisco IOS release trains with the IPS feature set enabled are vulnerable to the ATOMIC.TCP regular expression denial of service vulnerability:

- * 12.3T, except versions 12.3(2)T, 12.3(4)T, and 12.3(7)T
- * 12.3XQ, 12.3XR, 12.3XS, 12.3XW, 12.3XX, 12.3XY
- * 12.3YA, 12.3YD, 12.3YG, 12.3YH, 12.3YI, 12.3YJ, 12.3YK, 12.3YM, 12.3YQ, 12.3YS, 12.3YT, 12.3YX, 12.3YZ
- * 12.4
- * 12.4MR
- * 12.4T
- * 12.4XA, 12.4XB

To determine if the IPS feature set is active on an IOS device, use the "show ip ips configuration" command. This command will list the interfaces configured to use IPS inspection. You will then need to further check the status of each interface to confirm if they are enabled or not.

```
router#show ip ips configuration
Configured Config Locations: -none-
Last signature default load time: 18:46:50 UTC Jan 5 2007
Last signature delta load time: -none-
Last event action (SEAP) load time: -none-
IPS Auto Update is not currently configured
IPS fail closed is disabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through SDEE is enabled
Total Active Signatures: 85
Total Inactive Signatures: 61
IPS Rule Configuration
IPS name test
IPS Category CLI is not configured
Interface Configuration
Interface FastEthernet0/0
Inbound IPS rule is test
Outgoing IPS rule is not set
```

```
router#show ip interface FastEthernet0/0
```

[VulnWatch] Cisco Security Advisory: Multiple IOS IPS Vulnerabilities

FastEthernet0/0 is up, line protocol is up

In the above example, interface FastEthernet0/0 is configured to use IPS and is shown to be enabled.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability.

Details

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based feature that enables Cisco IOS software to mitigate network attacks. Cisco IOS IPS enables the network to defend itself with the intelligence to identify, classify, and stop or block certain malicious or damaging traffic in real time. The IOS IPS feature set contains multiple vulnerabilities. Only IOS images containing the IPS feature set are affected by these vulnerabilities.

Fragmented Packet Evasion Vulnerability

Some of the IPS signatures utilize regular expressions. Due to a vulnerability, an attacker can evade those IPS signatures by sending malicious network traffic as IP fragments. This may result in potential malicious traffic bypassing signature inspection and possibly allow the exploitation of protected systems. IPS signatures which do not utilize regular expressions are not affected by this vulnerability. All IP protocols (e.g. TCP, UDP, ICMP) are affected by this vulnerability. There is a mitigation for this vulnerability. This vulnerability is documented in Cisco Bug ID CSCsg15598.

ATOMIC.TCP Regular Expression Denial of Service Vulnerability

Certain network traffic can trigger IPS signatures which use the regular expression feature of the ATOMIC.TCP signature engine which may cause the IOS IPS device to crash. This may cause a denial of service resulting in disruption network traffic. Signature 3123.0 (Netbus Pro Traffic) has been demonstrated to trigger this vulnerability. There is a workaround for this vulnerability. This vulnerability is documented in Cisco Bug ID CSCsa53334.

Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory

[VulnWatch] Cisco Security Advisory: Multiple IOS IPS Vulnerabilities

based on the Common Vulnerability Scoring System (CVSS).

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

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

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

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>.

CSCsg15598 – DYIDS: Fragmentation prevents signature recognition

CVSS Base Score: 4.7

Access Vector: Remote

Access Complexity: Low

Authentication: Not Required

Confidentiality Impact: Partial

Integrity Impact: Partial

Availability Impact: None

Impact Bias: Normal

CVSS Temporal Score: 3.9

Exploitability: Functional

Remediation Level: Official Fix

Report Confidence: Confirmed

CSCsa53334 – bus error in single_pkt_regex

CVSS Base Score: 3.3

Access Vector: Remote

Access Complexity: Low

Authentication: Not Required

Confidentiality Impact: None

Integrity Impact: None

Availability Impact: Complete

Impact Bias: Normal

CVSS Temporal Score: 2

Exploitability: Functional

Remediation Level: Official Fix

Report Confidence: Confirmed

Impact

=====

Successful exploitation of the fragmented packet evasion vulnerability may result in an attacker being able to evade detection by an IOS IPS device. This could allow protected systems to be covertly attacked.

Successful exploitation of the ATOMIC.TCP regular expression denial of service vulnerability may cause an IOS IPS device to crash.

Software Version 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.

Each row of the Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL: <http://www.cisco.com/warp/public/620/1.html>

Major Release	Availability of Repaired Releases	Affected	12.3-Based	Rebuild	Maintenance	Release
All 12.3(2)T, 12.3(4)T, and 12.3(7)T						
releases are not vulnerable						

[VulnWatch] Cisco Security Advisory: Multiple IOS IPS Vulnerabilities

```
|-----|
| All 12.3(8)T releases are vulnerable |
|-----|
| 12.3(11)T10 ||
| 12.3T |-----+-----|
| 12.3(14)T7 ||
|-----|
| Limited platform support is available: |
| contact TAC |
|-----|
| Please migrate to 12.4(12) or later |
|-----+-----|
| 12.3XQ | Vulnerable; migrate to 12.4(12) or later |
|-----+-----|
| 12.3XR | Vulnerable; contact TAC |
|-----+-----|
| 12.3XS | Vulnerable; migrate to 12.4(12) or later |
|-----+-----|
| 12.3XW | Vulnerable; migrate to 12.3(11)YF or |
| later |
|-----+-----|
| 12.3XX | Vulnerable; migrate to 12.4(12) or later |
|-----+-----|
| 12.3XY | Vulnerable; migrate to 12.4(12) or later |
|-----+-----|
| 12.3YA | Vulnerable; contact TAC |
|-----+-----|
| 12.3YD | Vulnerable; migrate to 12.4(2)T3 or |
| later |
|-----+-----|
| 12.3YG | Vulnerable; migrate to 12.4(2)T3 or |
| later |
|-----+-----|
| 12.3YH | Vulnerable; migrate to 12.4(2)T3 or |
| later |
|-----+-----|
| 12.3YI | Vulnerable; migrate to 12.4(2)T3 or |
| later |
|-----+-----|
| 12.3YJ | Vulnerable; migrate to 12.3(14)YQ8 or |
| later |
|-----+-----|
| 12.3YK | Vulnerable; migrate to 12.4(4)T or later |
|-----+-----|
| 12.3YM | 12.3(14)YM5 ||
|-----+-----|
| 12.3YQ | 12.3(14)YQ8 ||
|-----+-----|
| 12.3YS | Vulnerable; migrate to 12.4(4)T or later |
|-----+-----|
| 12.3YT | Vulnerable; migrate to 12.4(4)T or later |
```

[VulnWatch] Cisco Security Advisory: Multiple IOS IPS Vulnerabilities

```
|-----|
| 12.3YX | 12.3(14)YX3 ||
|-----|-----|
| 12.3YZ | 12.3(11)YZ ||
|-----|-----|
| Affected ||
| 12.4-Based | Rebuild | Maintenance |
| Release ||
|-----|-----|
| | 12.4(1c) ||
|-----|-----|
| | 12.4(3b) | 12.4(5) |
|-----|-----|
| 12.4 | 12.4(7e); available ||
| 26-Mar-07 ||
|-----|-----|
| All 12.4(8) releases are vulnerable |
|-----|-----|
| | 12.4(10b) | 12.4(12) |
|-----|-----|
| 12.4MR | 12.4(6)MR1 ||
|-----|-----|
| | 12.4(2)T3 | 12.4(4)T |
|-----|-----|
| | | 12.4(6)T |
| 12.4T |-----|
| | 12.4(9)T3; available 9-Apr-07 |
|-----|-----|
| | 12.4(11)T1 |
|-----|-----|
| 12.4XA | 12.4(2)XA2 ||
|-----|-----|
| 12.4XB | 12.4(2)XB3 ||
|-----|-----|
| 12.4XE | Vulnerable; contact TAC |
|-----|
```

Workarounds

=====

The effectiveness of any mitigation 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 mitigation or fix is the most appropriate for use in the intended network before it is deployed.

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

[VulnWatch] Cisco Security Advisory: Multiple IOS IPS Vulnerabilities

<http://www.cisco.com/warp/public/707/cisco-air-20070213-iosips.shtml>

Fragmented Packet Evasion Vulnerability

There is a mitigation for the fragmented packet evasion vulnerability. The "fragments" keyword of IOS transit Access Control Lists (ACL) can be used to prohibit fragmented IP packets from transiting an IOS device. More information about filtering IP fragments can be found here:

* http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml#frag

Blocking IP fragments may have adverse affects on some protocols (like HTTP, FTP and Kerberos/Active Directory), so this workaround should be used with caution.

```
access-list 100 deny tcp any 10.1.1.0 0.0.0.255 fragments
access-list 100 deny udp any 10.1.1.0 0.0.0.255 fragments
```

ATOMIC.TCP Regular Expression Denial of Service Vulnerability

There is a workaround for the ATOMIC.TCP regular expression denial of service vulnerability by deleting IPS signature 3123.0 from the IOS IPS Signature Definition File (SDF). Disabling signature 3123.0 is alone not sufficient for the workaround to be effective. The following commands will delete signature 3123.0 from an IOS IPS device.

```
router#configure terminal
router(config)#ip ips signature 3123 delete
%IPS Signature 3123:0 is marked for deletion
%IPS The signature will be deleted when signatures are reloaded or saved
router(config)#interface FastEthernet0/0
router(config)#no ip ips test in
router(config)#ip ips test in
router(config)#exit
```

In the above example, signature 3123.0 is first deleted from the Signature Definition File, then the IPS instance running on interface FastEthernet0/0 is stopped and started to reinitialize the IPS state to reflect the signature deletion. If the IPS feature set is configured on multiple interfaces, then these steps must be completed for each affected interface.

To determine if signature 3123 is active, use the "show ip ips signature" command.

```
router#show ip ips signatures | include 3123
3123:0 N A MED 0 0 0 100 30 FA N S46
```

[VulnWatch] Cisco Security Advisory: Multiple IOS IPS Vulnerabilities

In the command output above, the N after 3123.0 indicates that the signature is present in the configuration but not enabled. Once the signature has been deleted, rerunning the "show ip ips signature" command shows:

```
router#show ip ips signatures | include 3123
3123:0 N* A MED 0 0 0 100 30 FA N S46
```

In the command output above, the N* after 3123.0 indicates that the signature has been deleted from the configuration. The IPS feature set must be restarted on each interface configured for IPS to complete the workaround. Once completed, the output of the "show ip ips signature" command will show:

```
router#show ip ips signatures | include 3123
```

```
router#
```

This vulnerability may affect any IPS signature using the regular expression functionality of the ATOMIC.TCP engine. Currently, Cisco only ships one signature configured this way (3123.0). If custom signatures have been added to an IOS IPS device configured use the ATOMIC.TCP engine with a regular expression, these signatures must also be deleted from the IPS configuration to ensure the effectiveness of the workaround.

Obtaining Fixed Software

=====

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@xxxxxxxx" or "security-alert@xxxxxxxx" 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 agreement 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 who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their 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@xxxxxxxx

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

=====

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

[VulnWatch] Cisco Security Advisory: Multiple IOS IPS Vulnerabilities

The fragmented packet evasion vulnerability was discovered internally by Cisco.

The ATOMIC.TCP regular expression denial of service vulnerability was reported to Cisco by a customer.

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.

Distribution

=====

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

<http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.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@xxxxxxxxxx
- * first-teams@xxxxxxxxxx
- * bugtraq@xxxxxxxxxxxxxxxxxxxxx
- * vulnwatch@xxxxxxxxxxxxxxxxxx
- * cisco@xxxxxxxxxxxxxxxxxxxxx
- * cisco-nsp@xxxxxxxxxxxxxxxxxxxxx
- * full-disclosure@xxxxxxxxxxxxxxxxxxxxx
- * comp.dcom.sys.cisco@xxxxxxxxxxxxxxxxxxxxx

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.

Revision History

=====

+-----+
| Revision 1.0 | 2007-February-13 | 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>.

All contents are Copyright 1992–2007 Cisco Systems, Inc. All rights reserved.

Updated: Feb 13, 2007 Document ID: 81545

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.2.2 (GNU/Linux)

iD8DBQFF0ekp8NUAbBmDaxQRAsjvAKCbqrL2lVQvVkTRzIa5R9KAj20BMACgrZsN
NIDbGQzvw+Cb3e4GebVhhgA=
=EdAD

-----END PGP SIGNATURE-----