

# Table of Contents

<b><u>Cisco Security Advisory: Cisco Security Agent Vulnerable to Crafted IP Attack</u></b> .....	1
<u>Document ID: 65545</u> .....	1
<u>Revision 1.0</u> .....	1
<u>For Public Release 2005 July 13 1600 UTC (GMT)</u> .....	1
<u>Please provide your feedback on this document</u> .....	1
<u>Summary</u> .....	1
<u>Affected Products</u> .....	1
<u>Vulnerable Products</u> .....	1
<u>Products Confirmed Not Vulnerable</u> .....	2
<u>Details</u> .....	2
<u>Impact</u> .....	2
<u>Software Versions and Fixes</u> .....	2
<u>Obtaining Fixed Software</u> .....	2
<u>Customers with Service Contracts</u> .....	2
<u>Customers using Third-party Support Organizations</u> .....	2
<u>Customers without Service Contracts</u> .....	3
<u>Workarounds</u> .....	3
<u>Exploitation and Public Announcements</u> .....	3
<u>Status of This Notice: FINAL</u> .....	3
<u>Distribution</u> .....	4
<u>Revision History</u> .....	4
<u>Cisco Security Procedures</u> .....	4

# Cisco Security Advisory: Cisco Security Agent Vulnerable to Crafted IP Attack

Document ID: 65545

## Revision 1.0

For Public Release 2005 July 13 1600 UTC (GMT)

---

Please provide your feedback on this document.

---

**Summary**  
**Affected Products**  
**Details**  
**Impact**  
**Software Versions and Fixes**  
**Obtaining Fixed Software**  
**Workarounds**  
**Exploitation and Public Announcements**  
**Status of This Notice: FINAL**  
**Distribution**  
**Revision History**  
**Cisco Security Procedures**

---

## Summary

Cisco Security Agent (CSA) is a network security software agent that provides threat protection for server and desktop computing systems.

A malicious attacker may be able to send a crafted IP packet to a Windows workstation or server running CSA 4.5 which may cause the device to halt and/or reload.

Repeated exploitation will create a sustained DoS (denial of service).

Cisco has made free software available to address this vulnerability.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID CSCsa85175 (registered customers only).

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20050713-csa.shtml>.

## Affected Products

### Vulnerable Products

Cisco CSA version 4.5 when running on any Microsoft Windows platforms except Windows XP.

## Products Confirmed Not Vulnerable

The following products are confirmed not vulnerable:

- Cisco CSA 4.0 and earlier
- Cisco CSA while running on Solaris
- Cisco CSA while running on Linux
- Cisco CSA while running on Windows XP

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

## Details

If a crafted IP packet with certain characteristics are sent to a Windows platform running CSA 4.5, Windows will halt with a blue screen and system crash.

When exploited, the affected machine will require a reboot to become operational again.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID CSCsa85175 (registered customers only) .

## Impact

Successful exploitation of this vulnerability will cause a reload of the affected machine.

## Software Versions and Fixes

This issue is fixed in CSA maintenance version 4.5.1.616 which is available for download at <http://www.cisco.com/cgi-bin/tablebuild.pl/csa>.

This issue is also fixed with CSA hotfix version 4.5.0.573 or later which is available for download at <http://www.cisco.com/cgi-bin/tablebuild.pl/csa/hf-crypto>.

A maintenance release is a scheduled revision of Cisco CSA that introduces new features or bug fixes, or both.

A hotfix is Cisco CSA update that delivers fixes on an accelerated schedule that introduce new bug fixes.

## Obtaining Fixed Software

### 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 assistance with the upgrade, which should be free of charge.

## 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@cisco.com](mailto:tac@cisco.com)

Please 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.

Please do not contact either "[psirt@cisco.com](mailto:psirt@cisco.com)" or "[security-alert@cisco.com](mailto:security-alert@cisco.com)" for software upgrades.

See <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.

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>.

## Workarounds

There are no recommended workarounds for this vulnerability. Please see the Obtaining Fixed Software section for appropriate solutions to resolve this vulnerability.

## Exploitation and Public Announcements

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

Cisco would like to thank Ben Collins at InfoSec Research Labs for bringing this to our attention.

## Status of This Notice: FINAL

THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE ADVISORY OR MATERIALS LINKED FROM THE ADVISORY IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS NOTICE AT ANY TIME.

A stand-alone copy or paraphrase of the text of this security advisory 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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20050713-csa.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-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [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.

## Revision History

Revision 1.0	2005 July 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](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 © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jul 15, 2005

Document ID: 65545

---