

# Cisco Security Advisory: Crafted Timed Attack Evades Cisco Security Agent Protections

Document ID: 63326

Advisory ID: cisco-sa-20041111-csa

<http://www.cisco.com/warp/public/707/cisco-sa-20041111-csa.shtml>

## Revision 1.2

**Last Updated** 2004 December 1 2130 UTC (GMT)

For Public Release 2004 November 11 1600 UTC (GMT)

---

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

---

[Summary](#)

[Affected Products](#)

[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

Cisco Security Agent (CSA) provides threat protection for server and desktop computing systems, also known as endpoints. It identifies and prevents malicious behavior, thereby eliminating known and unknown security risks.

A vulnerability exists in which a properly timed buffer overflow attack may evade the protections offered by CSA. The system under attack must contain an unpatched underlying vulnerability in system software that CSA is configured to protect. Another prerequisite for the attack is that a user must be interactively logged in during the attack.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20041111-csa.shtml>

Cisco is making patches available for CSA versions 4.0 free of charge, to correct the problem.

# Affected Products

This section provides details on affected products.

## Vulnerable Products

The following products are affected:

- Cisco Security Agent versions up to and excluding 4.0.3 build 728
- Cisco Security Agent 3.x versions
- Okena Stormwatch 3.x versions
- Cisco Security Agent for CallManager versions up to and excluding 4.0.3 build 728

### Determining the version of the CSA client

To determine which version of CSA is running on client machines simply right click on the CSA icon in the task bar. On the pop-up menu, selecting **About ...** will display the version number of the agent.

### Determining the version on the CSA Management Console

To determine which version of CSA you are running:

1. Log on to the Management console for Cisco Security Agent on your CiscoWorks server:  
`http://ciscoworks-hostname:1741/`
2. Select **VPN/Security Management Solution > Management Center > Security Agents**, and then click the **Security Agents** tab.

This will launch the **Management Center for Cisco Security Agents**. Within the browser window, locate the tab in the center marked **Help** and click on the sub-item labeled **About**. The version of the Cisco Security Agents should show up in a pop-up window containing text similar to **Management Center for Cisco Security Agents V4.0-1 build 540**

## Products Confirmed Not Vulnerable

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

## Details

CSA versions prior to 4.0.3.728 contain a vulnerability in the buffer overflow handling code allowing for the evasion of the protections offered by CSA. The evasion is timing dependent, where the second of two closely spaced overflow attacks is not processed by CSA.

In a vulnerable release a buffer overflow will trigger the Overflow heuristic, generating a query to the user. This query has a countdown timer of 5 minutes after which the default action of "Terminate" is taken in the event that the user does not make a selection. A second or subsequent buffer overflow attack that is received during this countdown period will not be trapped by CSA.

The result is that a sequence of two buffer overflow attacks in quick succession can result in the second bypassing CSA protection. If the attack is targeted at a vulnerable unpatched system process privileged access may result.

Agents prior to 4.0.3.728 are not affected if a user is not logged in or if the hidden GUI option is in effect.

Under these circumstances the agent knows that there is no user to respond to a query message. Because of this, the agent immediately takes the default action to terminate the process thus preventing the opportunity to evade the protection provided by CSA.

This has been documented in Cisco Bug ID [CSCef96160](#) ([registered](#) customers only).

## Impact

The integrity of the system which CSA is protecting may be compromised via privileged access which may be gained if patches for underlying system software vulnerabilities have not been applied.

## Software Versions and Fixes

Environments in which CSA is being used should ensure that they are running version [4.0.3.728](#) or later with a minimum of the default desktop or default server policy enabled.

Customers running Cisco Security Agent for CallManager should ensure that they are running version [CiscoCM-CSA-4.0.3.728-1.1.9](#) or later.

## Workarounds

Placing the agents into hidden user interface mode will cause agents to defeat this attack technique. This is configurable via the CSA Management Console by selecting **No user interaction** in all applicable groups for Microsoft Windows clients.

## Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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@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 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@cisco.com](mailto:tac@cisco.com)

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 aware of discussion of this vulnerability in a closed forum.

Customers running CSA should be aware that exploits do exist which could be used to exploit unpatched system software on machines where vulnerable versions of CSA are running.

## 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-20041111-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)

- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- 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 1.2	2004–December–1	Corrected URL in Summary section.
Revision 1.1	2004–November–19	Updated affected products and fixed software to include CSA agent fix on Cisco CallManager.
Revision 1.0	2004–November–11	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: Dec 01, 2004

Document ID: 63326

---