

[NT] Cisco Security Agent Vulnerable to Privilege Escalation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0095.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 11/30/05

To: list@securiteam.com

Date: 30 Nov 2005 09:55:49 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.secureteam.com/maillinglist.html>

Cisco Security Agent Vulnerable to Privilege Escalation

SUMMARY

Cisco Security Agent (CSA) is a security software agent that provides threat protection for server and desktop computing systems. CSA agents can be managed by CiscoWorks VMS Management Center for Cisco Security Agents or can be standalone agents running on Cisco IP Communications application servers. Standalone agents for Cisco IP Communications application servers must be manually installed on the IP Communications application server.

A vulnerability exists in CSA agents that can allow a privilege escalation through locally executed software, providing a normal user or attacker with local system level privileges on a Windows workstation or server running managed or standalone CSA 4.5.0 or 4.5.1 agents.

DETAILS

Affected Products:

Vulnerable Products:

CSA 4.5.0 and 4.5.1 agents managed by CiscoWorks VMS Management Center for Cisco Security Agents and standalone agents running on Cisco IP Communications application servers are affected when running on:

Securiteam: [NT] Cisco Security Agent Vulnerable to Privilege Escalation

* Microsoft Windows platforms including:

- o Windows 2003
- o Windows 2000 Server and Advanced Server
- o Windows NT v4.0 Server and Enterprise Server (SP 6a)
- o Windows NT 4 Workstation (SP 6a)
- o Windows 2000 Professional
- o Windows XP Professional

* Cisco CSA 4.5.0 (all builds) managed and standalone agents while running on Microsoft Windows

* Cisco CSA 4.5.1 (all builds) managed and standalone agents while running on Microsoft Windows

* Cisco CSA for CallManager versions 4.5.1 build 628 and 4.5.0 build 573.

Note: These versions are used by CallManager, Cisco Conference Connection (CCC), Emergency Responder, IPCC Express, IP Interactive Voice Response (IP IVR), and IP Queue Manager

* Cisco CSA for Intelligent Contact Management (ICM), IPCC Enterprise, and IPCC Hosted version 4.5.1 build 616

* Cisco CSA for Cisco Voice Portal (CVP) 3.0 and 3.1 version 4.5.0 build 573.

Note: This version is used by CVP 3.0 and 3.1 and CVP VXML Server.

Products Confirmed Not Vulnerable:

The following products are confirmed not vulnerable:

- * Cisco CSA 4.0.3 (all builds) and earlier managed and standalone agents
- * Cisco CSA 4.0.2 (all builds) and earlier managed and standalone agents
- * Cisco CSA 4.0.1 (all builds) and earlier managed and standalone agents
- * Cisco CSA 3.x versions
- * Okena Stormwatch 3.x versions
- * Cisco CSA agents running on Solaris
- * Cisco CSA agents running on Linux

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

Determining the CSA Client Version:

In order to determine which version of CSA is running on client machines, "right click" on the CSA icon in the Windows task bar. On the pop-up menu, selecting "About ..." will display the version number of the agent in a pop-up window containing text similar to "Cisco Security Agent V4.5 build 565."

Determining the CSA Client Version with the Management Console

You can also determine the CSA version using the Management Console for Cisco Security Agent on your CiscoWorks server. Complete these steps:

1. Login at:

<http://ciscoworks-hostname:1741/>

2. Select the "Security Agents" tab under:

Securiteam: [NT] Cisco Security Agent Vulnerable to Privilege Escalation

- * VPN/Security Management Solution
 - o Management Center
 - + Security Agents

This launches the "Management Center for Cisco Security Agents."

3. Within the browser window, locate the tab in the center marked "Help."
4. Click the sub-item labeled "About." The version of the Cisco Security Agents appears in a pop-up window containing text similar to:
Management Center for Cisco Security Agents V4.5-1 build 616.

Note: You can only manage CSA 4.5.X Agents with Version 4.5-X (any build) Management Center for Cisco Security Agents.

Details

Cisco Security Agent provides threat protection for server and desktop computing systems. Vulnerable versions of Cisco Security Agent may allow software executed locally to bypass systems protections and run with elevated privileges resulting in normal users and attackers obtaining local system level privileges.

Agent checks configured to prevent malicious software from running on a CSA protected system will be active; however, any checks that occur after successful exploitation may be bypassed.

This issue is not related to a Microsoft Operating System issue nor can a CSA policy modification change this behavior.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID CSCsc42373 (registered customers only)

For information about local system level privileges, refer to:

- * LocalSystem Account

<http://msdn.microsoft.com/library/en-us/dllproc/base/localsystem_account.asp>
http://msdn.microsoft.com/library/en-us/dllproc/base/localsystem_account.asp

Impact:

Successful exploitation of the vulnerability may result in a normal user or attacker gaining full control of the system, including the disabling of the CSA agent.

Software Versions and Fixes:

When considering software upgrades, also consult <<http://www.cisco.com/go/psirt>> <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

Securiteam: [NT] Cisco Security Agent Vulnerable to Privilege Escalation

release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

The fixed version of the Cisco Security Agent software requires no more resources than older 4.5.0 and 4.5.1 builds. It should be suitable for any system currently running 4.5.0 or 4.5.1.

* This issue is fixed in Management Center for Cisco Security Agents maintenance version 4.5.1.639.

o Download from:

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

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

o For installation and upgrade procedures:

<http://www.cisco.com/en/US/products/sw/secursw/ps5057/prod_installation_guides_list.html>

http://www.cisco.com/en/US/products/sw/secursw/ps5057/prod_installation_guides_list.html

* This issue is fixed in CSA for CallManager version 4.5.1.639.

o Download from:

<<http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>>

<http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>

o For installation and upgrade procedures:

Installing Cisco Security Agent for Cisco CallManager

Installing Cisco Security Agent for Cisco Customer Response Applications

Note: This version is used by CallManager, CCC, Emergency Responder, IPCC Express, IP IVR, and IP Queue Manager.

* This issue is fixed in CSA for ICM, IPCC Enterprise, and IPCC Hosted version 4.5.1.639.

o Download from:

<<http://www.cisco.com/cgi-bin/tablebuild.pl/csa10-crypto>>

<http://www.cisco.com/cgi-bin/tablebuild.pl/csa10-crypto>

o For upgrade procedures, refer to this document:

CiscoICM70-CSA-Installation-User-Guide.pdf, available at:

<<http://www.cisco.com/cgi-bin/tablebuild.pl/csa10-crypto>>

<http://www.cisco.com/cgi-bin/tablebuild.pl/csa10-crypto>

* This issue is fixed in CSA for CVP 3.0 and 3.1 version 4.5.1.639.

o Download from:

<<http://www.cisco.com/cgi-bin/tablebuild.pl/csa-cvp-20>>

<http://www.cisco.com/cgi-bin/tablebuild.pl/csa-cvp-20>

o For upgrade procedures, refer to this document:

CiscoCVP-CSA-InstallationGuide.pdf, available at:

<<http://www.cisco.com/cgi-bin/tablebuild.pl/csa-cvp-20>>

<http://www.cisco.com/cgi-bin/tablebuild.pl/csa-cvp-20>

Note: This version is used for CVP 3.0 and 3.1 and CVP VXML Server.

Securiteam: [NT] Cisco Security Agent Vulnerable to Privilege Escalation

Workarounds:

Workarounds for Cisco CSA 4.5.0 and 4.51 Managed Agents Running on Microsoft Windows

- * The risk of this issue can be mitigated by controlling the software allowed to run on workstations and servers.
- * Disabling or uninstalling the CSA agent is a workaround for this particular issue but leaves the workstation or server at risk to all other issues that the agent provides protection against. Disabling or uninstalling the CSA agent should only be considered as a last resort
- * There are no additional workarounds for this vulnerability. Please refer to the Obtaining Fixed Software section for appropriate solutions to resolve this vulnerability

Mitigation and Best Practices for Cisco CallManager and Voice Application Servers

- * The risk of this issue can be mitigated by controlling the software allowed to run on the server. Cisco strongly recommends configuring and using only the software that is approved to be installed on Cisco CallManager and Voice Application Servers.
- * IP telephony network security best practices can provide additional mitigation.
- * Cisco CallManagers and Voice Application servers should be on their own, separate IP networks
- * Cisco CallManagers and Voice Application servers should be protected at layer 2.
- * Access controls should be employed to protect voice networks from attacks that may originate from the data network.
- * Follow Operating System hardening best practices for Cisco CallManagers and Voice Application servers.
- * Implement approved Anti-Virus software on Cisco CallManagers and voice application servers.
- * For additional information about IP telephony network security best practices refer to:
IP Telephony SRND for Cisco CallManager 3.3

Workarounds for Systems Protected by Standalone CSA Agents Cisco CSA for CallManager, CCC, Emergency Responder, IPCC Express, IP IVR, and IP Queue Manager

- * Downgrade to Cisco CSA for CallManager version 4.0.3 build 728 which is available for download at:
<<http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>>
<http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>
- * Disabling or uninstalling the CSA agent is a workaround this particular issue but leaves the workstation or server at risk to all other issues that the agent provides protection against. Disabling or uninstalling the CSA agent should only be considered as a last resort.
- * Procedures to uninstall and install CSA for CallManager can be found in the following documents:
Installing Cisco Security Agent for Cisco CallManager
Installing Cisco Security Agent for Cisco Customer Response Applications

Securiteam: [NT] Cisco Security Agent Vulnerable to Privilege Escalation

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

Cisco CSA for ICM, IPCC Enterprise, and IPCC Hosted Version 4.5.1 build 616

* Disabling or uninstalling the CSA agent is a workaround this particular issue but leaves the workstation or server at risk to all other issues that the agent provides protection against. Disabling or uninstalling the CSA agent should only be considered as a last resort.

* Uninstall procedures can be found in the following document: CiscoICM70-CSA-Installation-User-Guide.pdf which is available at:

<<http://www.cisco.com/cgi-bin/tablebuild.pl/csa10-crypto>>
<http://www.cisco.com/cgi-bin/tablebuild.pl/csa10-crypto>

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

Cisco CSA for CVP 3.0 and 3.1 version 4.5.0 build 573. This version is used by CVP 3.0 and 3.1 and CVP VXML Server

* Disabling or uninstalling the CSA agent is a workaround this particular issue but leaves the workstation or server at risk to all other issues that the agent provides protection against. Disabling or uninstalling the CSA agent should only be considered as a last resort.

* Uninstall procedures can be found in the following document:

CiscoCVP-CSA-InstallationGuide.pdf which is available at:

<<http://www.cisco.com/cgi-bin/tablebuild.pl/csa-cvp-20>>
<http://www.cisco.com/cgi-bin/tablebuild.pl/csa-cvp-20>

* There are no additional workarounds for this vulnerability. Please refer to the Obtaining Fixed Software section for appropriate solutions to resolve this vulnerability.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt@cisco.com>> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20051129-csa.shtml>>
<http://www.cisco.com/warp/public/707/cisco-sa-20051129-csa.shtml>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

Securiteam: [NT] Cisco Security Agent Vulnerable to Privilege Escalation

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.