

[UNIX] Cisco Security Agent for Linux Port Scan DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-10/msg00096.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 25 Oct 2006 21:12:41 +0200
-

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Cisco Security Agent for Linux Port Scan DoS

SUMMARY

Cisco Security Agent (CSA) for Linux contains a denial of service vulnerability involving port scans. By performing a port scan against a system running a vulnerable version of CSA, it is possible to cause the system to become unresponsive. Cisco Unified CallManager (CUCM) and Cisco Unified Presence Server (CUPS) ship with a vulnerable CSA version.

There are workarounds for this vulnerability. Cisco has made free software available to address this vulnerability for affected customers.

DETAILS

Vulnerable Products:

- The following CSA versions are vulnerable to the port scanning issue:
- * CSA version 4.5 for Linux (standalone and managed) prior to Hotfix 4.5.1.657
 - * CSA version 5.0 for Linux (standalone and managed) prior to Hotfix 5.0.0.193

The following Cisco products include a standalone CSA for Linux version

[UNIX] Cisco Security Agent for Linux Port Scan DoS

which are also vulnerable to this issue:

- * Cisco Unified CallManager (CUCM) 5.0 versions including 5.0(4)
- * Cisco Unified Presence Server (CUPS) 1.0 versions including 1.0(2)

Products Confirmed Not Vulnerable:

The following CSA Agent versions are not vulnerable to the port scanning issue:

- * CSA version 5.1 (standalone and managed) for Linux
- * All CSA versions (standalone and managed) for Windows
- * All CSA versions (standalone and managed) for Solaris

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

Details:

Cisco Security Agent (CSA) provides threat protection for server and desktop computing systems. CSA for Linux is vulnerable to a denial of service attack that may be triggered during the identification of network port scans. By running a port scan with specific options, it is possible to cause excessive system resource consumption resulting in a denial of service. It is possible to mitigate this vulnerability by restricting network access to vulnerable systems to trusted networks. This issue is not a Linux operating system i