

Cisco Security Advisory: Cisco Security Manager Vulnerability

Advisory ID: cisco-sa-20090121-csm

<http://www.cisco.com/warp/public/707/cisco-sa-20090121-csm.shtml>

Revision 1.0

For Public Release 2009 January 21 1600 UTC (GMT)

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

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring 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 Manager contains a vulnerability when it is used with Cisco IPS Event Viewer (IEV) that results in open TCP ports on both the Cisco Security Manager server and IEV client. An unauthenticated, remote attacker could leverage this vulnerability to access the MySQL databases or IEV server.

Cisco has released free software updates that address this vulnerability. A workaround is also available to mitigate this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090121-csm.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

All 3.1 and 3.2 versions prior to 3.2.2 of Cisco Security Manager are affected by this vulnerability. Cisco IEV is installed with Cisco Security Manager by default, but the vulnerability is not exposed until IEV has been launched.

☐ Products Confirmed Not Vulnerable

The following products have been confirmed not vulnerable:

- Cisco Security Manager 3.2.2
- Cisco Security Manager 3.0.x and earlier
- Standalone implementations of Cisco IEV
- Cisco IPS Manager Express

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

[Top of the section](#) [Close Section](#)

☐ Details

Cisco Security Manager is an enterprise-class management application that is designed to configure

firewall, VPN, and intrusion prevention security services on Cisco network and security devices. As part of Cisco Security Manager installation, the Cisco IEV is installed by default. The IEV is a Java-based application that allows users to view and manage alerts for up to five sensors, including the ability to report top alerts, attackers, and victims over a specified number of hours or days. Users can connect to and view alerts in real time or via imported log files, configure filters and views to help manage alerts, and import and export event data for further analysis.

A vulnerability exists in the Cisco Security Manager server. When the IEV is launched, it opens several remotely available TCP ports on the Cisco Security Manager server and client. These ports could allow remote, unauthenticated root access to the IEV database and server. When IEV is closed, it closes open ports on the Cisco Security Manager client that launched the IEV but fails to close open ports on the server. If the IEV has never been used on the system, the Cisco Security Manager server is not vulnerable.

The IEV database contains events that are collected from Cisco Intrusion Prevention System (IPS) devices. The IEV server allows an unauthenticated user to add, delete, or modify the devices that are added into the IEV.

This vulnerability is documented in Cisco Bug ID: [CSCsv66897](#) ([registered](#) customers only)

This vulnerability have been assigned the Common Vulnerabilities and Exposures (CVE) identifiers CVE-2008-3820.

[Top of the section](#) [Close Section](#)

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

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

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

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> .

CSCsv66897: Cisco Security Manager/IEV: TCP Ports open for remote connection without any authentication					
Calculate the environmental score of CSCsv66897					
CVSS Base Score - 8.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Complete	Complete	None
CVSS Temporal Score - 7.3					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#) [Close Section](#)

☐ Impact

Successful exploitation of this vulnerability may result in remote root access to the IEV database or to the IEV Server. Upon launching the IEV remotely accessible ports are opened on the Cisco Security Manager server and the client where the IEV is launched. When the IEV application is closed these ports are subsequently closed on the client however remain open on the Cisco Security Manager server;

[Top of the section](#) [Close Section](#)

☐ Software Versions 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.

A software patch for Cisco Security Manager versions 3.1, 3.1.1, 3.2 and 3.2.1 is available for download at: <http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app?psrtdcat20e2>

The patch file names by Cisco Security Manager version follow:

Cisco Security Manager version	Patch Filename
3.0.x and earlier	Not Vulnerable
3.1	CSM310PatchCSCsv66897.zip
3.1.1.SP3	CSM311SP3PatchCSCsv66897.zip
3.2.SP2	CSM320SP2PatchCSCsv66897.zip
3.2.1.SP1	CSM321SP1PatchCSCsv66897.zip
3.2.2	Not Vulnerable

Please read the corresponding readme files for installation instructions.

[Top of the section](#) [Close Section](#)

Workarounds

In the event that Cisco IEV is not being used, administrators are advised to disable the functionality until a patch is applied. To disable IEV on Cisco Security Manager, perform the following steps:

1. Access the Microsoft Windows Server that Cisco Security Manager is installed on.
2. Open the Services dialog box (Choose **Start > Administrative Tools > Services**).
3. Locate the Cisco IPS Event Viewer service and open Properties.
4. Change **Startup Type:** to **Disabled** and click **Ok**.
5. Stop the Cisco IPS Event Viewer service.

6. Stop and Restart the Cisco Security Manager Daemon Manager service.
7. Confirm that the Cisco IPS Event Viewer service has not restarted.

Upon disabling the Cisco IPS Event Viewer service, the open ports on the Cisco Security Manager server will be closed.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory: <http://www.cisco.com/warp/public/707/cisco-amb-20090121-csm.shtml>

[Top of the section](#) [Close Section](#)

☐ **Obtaining Fixed Software**

Cisco has released free software updates that address these vulnerabilities. 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/en/US/docs/general/warranty/English/EU1KEN_.html, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml> .

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

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

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

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

This vulnerability was discovered through internal Cisco testing.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

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

<http://www.cisco.com/warp/public/707/cisco-sa-20090121-csm.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
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- 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.

[Top of the section](#) [Close Section](#)

☐ **Revision History**

Revision 1.0	2009-January-21	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>.

Help us help you.



Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor



This document solved my problem.

- Yes
- No
- Just browsing



Suggestions for improvement:

(256 character limit)



[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)