Table of Contents

Cisco Security Advisory: Cisco IPS MC Malformed Configuration Download Vulnerability

Document ID: 68065

Revision 1.0

Last Updated

For Public Release 2005 November 1 2000 UTC (GMT)

Please provide your feedback on this document.

Summary

The CiscoWorks VPN/Security Management Solution (VMS) is a network management application that includes Web−based tools for configuring, monitoring, and troubleshooting VPNs, firewalls, network intrusion detection systems (NIDSs), network intrusion prevention systems (NIPSs) and host intrusion prevention systems (HIPSs). CiscoWorks VMS also includes network device inventory, change audit, and software distribution features.

An issue exists in one of the components of the Cisco Management Center for IPS Sensors (IPS MC) v2.1 during the generation of the Cisco IOS IPS (Intrusion Prevention System) configuration file that may result in some signatures belonging to certain classes being disabled during the configuration deployment process.

Cisco has made a free software patch available to address this vulnerability for affected customers.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco−sa−20051101−ipsmc.shtml.

Affected Products

Vulnerable Products

- Cisco IOS IPS devices that have been configured by IPS MC v2.1.

Products Confirmed Not Vulnerable

- Cisco IOS IPS devices that have NOT been configured by IPS MC v2.1. This category includes Cisco IOS IPS devices that have been configured by using any of the following methods:
    - ♦ Cisco IDS MC (Management Center for IDS Sensors)
    - ♦ Cisco SDM (Security Device Manager)
    - ♦ Cisco IOS CLI (Command Line Interface)
- Any other Cisco IDS/IPS solution, configured by either Cisco IPS MC v2.1, Cisco IDS MC (any version), Cisco SDM (any version) or by using the Cisco IOS CLI. These include:
    - ♦ Cisco IOS IDS
    - ♦ Cisco PIX/ASA IDS
    - ♦ Cisco IPS 4200 Series Sensors
    - ♦ Cisco Catalyst 6500/7600 Series Intrusion Detection System (IDSM−2) Module
    - ♦ Cisco IDS Network Module (NM−CIDS−K9)
    - ♦ Cisco ASA Advanced Inspection and Prevention (AIP) Security Services Module

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

Details

Some Cisco routers running Cisco IOS include a feature called Cisco IOS IPS. The Cisco IOS IPS acts as an in−line intrusion protection sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures that have been enabled on the device configuration. When it detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE). The network administrator can configure Cisco IOS IPS to choose the appropriate response to various threats.

Customers can use multiple methods, including Cisco IPS MC, Cisco IDS MC, Cisco SDM and the Cisco IOS CLI, to enable, disable and configure Cisco IOS IPS signatures. Some signatures dealing with TCP or UDP traffic analyze traffic destined to specific ports. Those ports are pre−configured with default values, and some signatures might allow changes to the list of ports to be monitored.

If the Cisco IOS IPS devices have been configured by using the Cisco IPS MC v2.1, the Cisco IPS MC might download a configuration file to the device that does not contain a value for the port field in one or more signatures, resulting in the affected Cisco IOS IPS device disabling those signatures. Only signatures using either the STRING.TCP or STRING.UDP signature micro−engine (SME) are affected by this vulnerability. Additionally, this behavior only happens if those signatures were enabled and configured from the Cisco IPS MC GUI ; signatures belonging to the STRING.TCP or STRING.UDP SMEs that were previously configured on the device and imported into the Cisco IPS MC will not experience this issue.

The list of signatures currently loaded into a Cisco IOS IPS device and their status can be obtained by executing the **show ip ips signatures** command. The following abbreviated output shows signatures currently loaded into the device, both enabled and disabled:

```
Router#show ip ips signatures
Builtin signatures are configured
Signatures were last loaded from flash:128MB.sdf

Cisco SDF release version 128MB.sdf v4

Trend SDF release version V0.0

*=Marked for Deletion  Action=(A)larm,(D)rop,(R)eset   Trait=AlarmTraits
MH=MinHits             AI=AlarmInterval               CT=ChokeThreshold
```

```
TI=ThrottleInterval    AT=AlarmThrottle                FA=FlipAddr
WF=WantFrag

Signature Micro-Engine: OTHER (4 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Version
 ---------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- -------
  1201:0      Y   A    HIGH     0      0     0    30    15 FA  N  N 2.2.1.5
  1202:0      Y   A    HIGH     0      0     0   100    15 FA  N  N 2.2.1.5
  1203:0      Y   A    HIGH     0      0     0    30    15 FA  N  N 2.2.1.5
  3050:0      Y   A    HIGH     0      0     0     0    15 FA  N    1.0

Signature Micro-Engine: STRING.ICMP (1 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Version
 ---------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- -------
  2156:0      Y   A     MED     0      0     0     0    15 FA  N    S54

Signature Micro-Engine: STRING.UDP (16 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Version
 ---------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- -------
  4060:0      Y   A     MED     0      0     0     0    15 FA  N    S10
  4060:1      Y   A     MED     0      0     0     0    15 FA  N    S173
  4607:0      Y   A    HIGH     0      0     0     0    15 FA  N    S30
  4607:1      Y   A    HIGH     0      0     0     0    15 FA  N    S30
  4607:2      Y   A    HIGH     0      0     0     0    15 FA  N    S30
  4607:3      Y   A    HIGH     0      0     0     0    15 FA  N    S30
  4607:4      Y   A    HIGH     0      0     0     0    15 FA  N    S30
  4608:0      N   A    HIGH     0      1     0     0    15 FA  N    S30
  4608:1      Y   A    HIGH     0      1     0     0    15 FA  N    S30
  4608:2      Y   A    HIGH     0      1     0     0    15 FA  N    S30
 11000:0      N   A     LOW     0      0     0     0    15 FA  N    S37
 11000:1      Y   A     LOW     0      0     0     0    15 FA  N    S37
 11000:2      Y   A     LOW     0      0     0     0    15 FA  N    S136
 11207:0      Y   A    INFO     0      0     0     0    15 FA  N    S139
 11208:0      Y   A    INFO     0      0     0     0    15 FA  N    S139
 11209:0      Y   A    INFO     0      0     0     0    15 FA  N    S139

Signature Micro-Engine: STRING.TCP (60 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Version
 ---------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- -------
  3116:0      Y   A    HIGH     0      1     0     0    15 FA  N    S12
  3117:0      N   A     LOW     0      1     0     0    15 FA  N    S13
  3117:1      Y   A     LOW     0      1     0     0    15 FA  N    S13
  3120:0      Y   A     LOW     0      1     0     0    15 FA  N    S13
  3120:1      Y   A     LOW     0      1     0     0    15 FA  N    S13
  3132:0      Y   A    HIGH     0      1     0     0    15 FA  N    S67
  3132:1      Y   A    HIGH     0      1     0     0    15 FA  N    S67
  3135:0      Y   A    HIGH     0      1     0     0    15 FA  N    S73
  3137:1      Y   A    HIGH     0      1     0     0    15 FA  N    S83
  3137:2      Y   A    HIGH     0      1     0     0    15 FA  N    S128
  3141:0      Y   A    HIGH     0      1     0     0    15 FA  N    S94
  3142:1      Y   A    HIGH     0      1     0     0    15 FA  N    S92
  3152:0      Y   A     MED     0      1     0     0    15 FA  N    2.1.1
  3450:0      Y   A     LOW     0      1     0     0    15 FA  N    1.0
  5570:0      Y   A R  HIGH     0      1     0     0    15 FA  N    S185
  5571:0      Y   A R  HIGH     0      1     0     0    15 FA  N    S185
  9479:0      Y   A    HIGH     0      1     0     0    15 FA  N    S104
  9480:0      Y   A    HIGH     0      1     0     0    15 FA  N    S104
  9481:0      Y   A    HIGH     0      1     0     0    15 FA  N    S104
  9482:0      Y   A    HIGH     0      1     0     0    15 FA  N    S104
  9483:0      Y   A    HIGH     0      1     0     0    15 FA  N    S104
 --More--
```

Any signature with a capital N under the 'On' column is DISABLED, while any signature with a capital Y under the same column is ENABLED. In this example, signatures 4608:0 and 11000:0 (belonging to the STRING.UDP SME), and signature 3117:0 (belonging to the STRING.TCP SME) are listed as disabled. For each signature listed as disabled in the output of the **show ip ips signatures** command, a corresponding **ip ips signature <SigID> <SubsigID> disable** command should be visible on the running configuration. This is an example of the **show running−configuration** command, using a filter to only display configuration lines belonging to signatures that have been disabled:

```
Router#show running-config | include ip ips signature .* disable
ip ips signature 11000 0 disable
ip ips signature 4608 0 disable
ip ips signature 3117 0 disable
Router#
```

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID CSCsc33696 (registered customers only)

Impact

While this is not a vulnerability in the Cisco IOS IPS code itself, in the processing performed by Cisco IOS IPS on traffic traversing the device, or in the Cisco IPS MC v2.1, this vulnerability might result in an incomplete analysis of network traffic traversing the Cisco IOS IPS device, which could allow some attacks to go unnoticed.

Software Versions and Fixes

When considering software upgrades, please also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html 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") for assistance.

Cisco has developed a software fix for this vulnerability. Once the fix is applied to a VMS server running IPS MC v2.1, the IPS MC will correctly populate the port field attached to a signature using either the STRING.TCP or STRING.UDP SME. Additional steps will be required to be performed. Please read the README file published together with the software fix.

In order to obtain this software fix, customers should access the VMS Software download page for IDS MC and IPS MC, available at http://www.cisco.com/cgi−bin/tablebuild.pl/mgmt−ctr−ids−app. The fix consists of the following three files:

- **idsmdc2.1.0−win−CSCsc336961.tar** − this file contains the fix itself for IPS MC v2.1 running on the Windows operating system.
- **CSCOids2.1.0−sol−CSCsc336961.tar** − this file contains the fix itself for IPS MC v2.1 running on the Solaris operating system.
- **CSCsc33696−README.txt** − this file contains instructions on how to apply the software fix to an affected IPS MC v2.1 installation (either Windows or Solaris) and any needed pre and post installation tasks to be carried out by the user.

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

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" or "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.

This vulnerability was reported to Cisco by a customer.

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 is posted on Cisco's worldwide website at http://www.cisco.com/warp/public/707/cisco−sa−20051101−ipsmc.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−teams@first.org (includes CERT/CC)
- 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.

Revision History

Revision 1.0	2005−November−1	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.

Updated: Nov 01, 2005 Document ID: 68065