Cisco IOS IPS Support for Microsoft Engines

Last Updated: August 14, 2012

The Cisco IOS IPS Support for Microsoft Engines feature extends Cisco IOS Intrusion Prevention Systems (IPS) to support Microsoft RPC (Remote Procedure Call) and Microsoft SMB (Server Message Block) protocols. IPS signatures can now scan for, detect, and take proper action against vulnerabilities in MSRPC and SMB protocols.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Cisco IOS IPS Support for Microsoft Engines

Cisco IOS IPS Overview

The Cisco IOS IPS acts as an in-line intrusion prevention sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. 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. The Signature Event Action Processor (SEAP) can dynamically control actions that are to be taken by a signature event on the basis of parameters such as fidelity, severity, or target value rating. These parameters have default values but can also be configured via CLI. When packets in a session match a signature, Cisco IOS IPS can take any of the following actions, as appropriate:

- Send an alarm to a syslog server or a centralized management interface
- Drop the packet
- Reset the connection
- Deny traffic from the source IP address of the attacker for a specified amount of time
- Deny traffic on the connection for which the signature was seen for a specified amount of time

Cisco developed its Cisco IOS software-based intrusion-prevention capabilities and Cisco IOS Firewall with flexibility in mind, so that individual signatures could be disabled in case of false positives. Generally, it is preferable to enable both the firewall and Cisco IOS IPS to support network security policies. However, each of these features may be enabled independently and on different router interfaces.

How to Use Cisco IOS IPS

The addition of the MSRPC and MSB protocol support does not change the way in which Cisco IOS IPS is defined and enabled in your network. For information on how to enable IPS on your network via command-line interface (CLI), see the section “How to Use Cisco IOS 5.x Format Signatures with Cisco IOS IPS” within the document *Cisco IOS IPS 5.x Signature Format Support and Usability Enhancement*.

Configuration Examples for Cisco IOS IPS

show ip ips signature Output to Verify MS Engines Example

The following sample output from the **show ip ips signature** command displays output for the service-msrpc and service-smb-advanced signatures:

```
Signature Micro-Engine: service-msrpc: Total Signatures 21
service-msrpc enabled signatures: 21
service-msrpc compiled signatures: 21
SigID:SubID En Cmp Action Sev Trait EC AI GST SI SM SW SFR Rel
----------- -- ---- ------ --- ----- ---- ---- ----- --- -- -- --- ---
3330:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S148
3332:0 Y Y A HIGH 0 35 0 0 0 FA N 100 S148
3337:0 Y Y A HIGH 0 8 2 0 0 FA N 100 S85
3331:2 Y Y A HIGH 0 1 0 0 0 FA N 90 S215
3327:12 Y Y A HIGH 0 1 0 0 0 FA N 85 S214
3328:3 Y Y A MED 0 1 0 0 0 FA N 85 S170
3328:1 Y Y A MED 0 1 0 0 0 FA N 85 S148
3327:8 Y Y A INFO 0 1 0 0 0 FA N 85 S214
3334:6 Y Y A HIGH 0 1 0 0 0 FA N 80 S215
3327:0 Y Y A HIGH 0 1 0 0 0 FA N 80 S165
6232:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S209
3327:4 Y Y A HIGH 0 1 0 0 0 FA N 75 S188
3334:5 Y Y A HIGH 0 2 2 0 0 FA N 75 S179
3338:2 Y Y A HIGH 0 40 3 0 0 FA N 75 S175
```

```
3338:3 Y Y A HIGH 0 1 0 0 0 FA N 75 S175
6130:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S167
6130:6 Y Y A INFO 0 1 0 0 0 FA N 75 S192
5567:1 Y Y A INFO 0 1 0 0 0 FA N 55 S187
5567:2 Y Y A INFO 0 1 0 0 0 FA N 55 S187
5567:3 Y Y A INFO 0 1 0 0 0 FA N 55 S187
5567:4 Y Y A INFO 0 1 0 0 0 FA N 55 S187
Signature Micro-Engine: service-smb-advanced: Total Signatures 31
service-smb-advanced enabled signatures: 31
service-smb-advanced compiled signatures: 31
SigID:SubID En Cmp Action Sev Trait EC AI GST SI SM SW SFR Rel
----------- -- ---- ------ --- ----- ---- ---- ----- --- -- -- --- ---
5593:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S262
5592:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S262
5582:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S262
5599:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S262
5595:0 Y Y A MED 0 1 0 0 0 FA N 100 S262
5579:0 Y Y A INFO 0 1 0 0 0 FA N 100 S264
5581:0 Y Y A INFO 0 1 0 0 0 FA N 100 S264
5580:0 Y Y A INFO 0 1 0 0 0 FA N 100 S264
5584:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5576:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5577:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5583:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5591:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5590:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5598:0 Y Y A HIGH 0 1 0 0 0 FA N 85 S264
5588:0 Y Y A HIGH 0 1 0 0 0 FA N 85 S262
5586:0 Y Y A HIGH 0 1 0 0 0 FA N 85 S262
5585:0 Y Y A MED 0 1 0 0 0 FA N 85 S264
5579:1 Y Y A MED 0 1 0 0 0 FA N 85 S264
5602:0 Y Y A MED 0 1 0 0 0 FA N 85 S262
5589:0 Y Y A LOW 0 1 0 0 0 FA N 85 S262
5578:0 Y Y A INFO 0 1 0 0 0 FA N 85 S264
5605:0 Y Y A INFO 0 1 0 0 0 FA N 85 S262
5600:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S262
5597:0 Y Y A HIGH 0 50 0 0 0 FA N 75 S262
5594:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S262
5587:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S262
5603:0 Y Y A MED 0 1 0 0 0 FA N 75 S262
5591:1 Y Y A INFO 0 1 0 0 0 FA N 75 S262
5575:0 Y Y A INFO 0 1 0 0 0 FA N 75 S262
5590:1 Y Y A INFO 0 1 0 0 0 FA N 75 S262
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco IOS IPS Support for Microsoft Engines

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Cisco IOS IPS Support for Microsoft Engines

Feature Name	Releases	Feature Information
Cisco IOS IPS Support for Microsoft Engines	12.4(15)T	The Cisco IOS IPS Support for Microsoft Engines feature extends Cisco IPS to support MSRPC and SMB protocols. The following commands were introduced or modified: **debug ip ips**