

[NEWS] Cisco IPS Privilege Escalation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0100.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/28/05

To: list@securiteam.com

Date: 28 Aug 2005 10:26:00 +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 IPS Privilege Escalation

SUMMARY

<<http://www.cisco.com/en/US/products/sw/secursw/ps2113/>> Cisco Intrusion Prevention Systems (IPS) are a family of network security devices that provide network based threat prevention services.

A user with OPERATOR or VIEWER access privileges may be able to exploit a vulnerability in the command line processing (CLI) logic to gain full administrative control of the IPS device.

DETAILS

Vulnerable Systems:

- * Cisco Intrusion Prevention System version 5.0(1) and 5.0(2)

Immune Systems:

- * Cisco Intrusion Detection Systems (IDS) or IPS version 4.x and prior
- * Cisco IPS version 5.0(3)

A user with OPERATOR or VIEWER access privileges may be able to exploit a vulnerability in the command line processing logic to gain full administrative control of the IPS device. OPERATOR and VIEWER accounts are normally non-privileged accounts used for monitoring and troubleshooting

Securiteam: [NEWS] Cisco IPS Privilege Escalation

purposes.

Successful exploitation of this vulnerability grants an attacker full control of the IPS Device.

With full administrative access, an attacker may use the IPS device to bypass intrusion detection logic, run arbitrary code or perform a denial of service attack on the network and/or IPS device.

If the IPS device is used in inline mode, an attacker may cause an interruption of network service.

Vendor Status:

The vendor has issues a fix at:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ips5> IPS version 5.0(3)

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-20050824-ips.shtml>
<http://www.cisco.com/warp/public/707/cisco-sa-20050824-ips.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

=====

=====

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.