

[NEWS] Cisco Internetwork Operating System IPv6 DoS and Arbitrary Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0006.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/01/05

To: list@securiteam.com

Date: 1 Aug 2005 18:44:20 +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 Internetwork Operating System IPv6 DoS and Arbitrary Code Execution

SUMMARY

IPv6 is the "Internet Protocol Version 6", designed by the Internet Engineering Task Force (IETF) to replace the current version Internet Protocol, IP Version 4 (IPv4).

Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

DETAILS

Vulnerable Systems:

A list of vulneable systems can be found at:

<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml#software>

<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml#software>

Technical Details:

Securiteam: [NEWS] Cisco Internetwork Operating System IPv6 DoS and Arbitrary Code Execution

A vulnerability exists in the processing of IPv6 packets. Crafted packets from the local segment received on logical interfaces (that is, tunnels including 6to4 tunnels) as well as physical interfaces can trigger this vulnerability. Crafted packets can not traverse a 6to4 tunnel and attack a box across the tunnel.

The crafted packet must be sent from a local network segment to trigger the attack. This vulnerability can not be exploited one or more hops from the IOS device.

This issue affects all Cisco devices running any unfixed version of Cisco IOS or Cisco IOS XR code that supports, and is configured for, IPv6. A system which supports IPv6, if not specifically configured for IPv6, is not affected. You can use the show ipv6 interface command to determine whether IPv6 is enabled on a system.

Successful exploitation of the vulnerability on Cisco IOS may result in a reload of the device or execution of arbitrary code. Repeated exploitation could result in a sustained DoS attack or execution of arbitrary code on Cisco IOS devices.

Successful exploitation of the vulnerability on Cisco IOS–XR may result in a restart of the IPv6 neighbor discovery process. A restart of this process will only affect IPv6 traffic passing through the system. All other processes and traffic will be unaffected. Repeated exploitation could result in a sustained DoS attack on IPv6 traffic.

Example:

Sample output of the show ipv6 interface command is shown below for two systems, one not configured for IPv6 and one configured for IPv6.

An empty output or an error message will be displayed if IPv6 is disabled or unsupported on the system.

```
Router#show ipv6 int fa 0/0
–here you see blank output
```

In the example below the system is vulnerable.

```
Router#show ipv6 interface
Serial1/0 is up, line protocol is up
IPv6 is enabled, link–local address is FE80::A8BB:CCFF:FE00:D200
Global unicast address(es):
  2001:1:33::3, subnet is 2001:1:33::/64
Joined group address(es):
  FF02::1
  FF02::1:FF00:3
  FF02::1:FF00:D200
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
```

Securiteam: [NEWS] Cisco Internetwork Operating System IPv6 DoS and Arbitrary Code Execution

ND reachable time is 30000 milliseconds

Router#

A router that has IPv6 enabled on a physical or logical interface is vulnerable to this issue even if ipv6 unicast-routing is globally disabled. The show ipv6 interface command can be used to determine whether IPv6 is enabled on any interface.

To determine the software running on a Cisco product, log in to the device and issue the show version command to display the system banner. Cisco IOS Software will identify itself as "Internetwork Operating System Software" or simply "IOS." On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the show version command or will give different output.

The following example shows a product running IOS release 12.3(6) with an image name of C2600-JS-MZ:

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.3(6), RELEASE SOFTWARE (fc1)
```

Additional information about Cisco IOS release naming can be found at
<<http://www.cisco.com/warp/public/620/1.html>>
<http://www.cisco.com/warp/public/620/1.html>.

A system that is running a Cisco IOS XR version prior to 3.2 is also affected by this vulnerability if configured for IPv6. The show ipv6 interface command can be used to identify whether IPv6 is enabled on a system running Cisco IOS XR.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt@cisco.com>> Cisco.com.
The original article can be found at:
<<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>>
<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.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.