

# [NEWS] Cisco IOS Heap-based Overflow Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0017.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 11/06/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 6 Nov 2005 13:25:06 +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 IOS Heap-based Overflow Vulnerability

---

## SUMMARY

<[http://www.cisco.com/en/US/products/ps6537/products\\_ios\\_sub\\_category\\_home.html](http://www.cisco.com/en/US/products/ps6537/products_ios_sub_category_home.html)> Cisco IOS (originally Internetwork Operating System) is the operating system used on Cisco Systems routers and some network switches (those which do not use CatOS). It is a multitasking operating system and provides kernel services such as process scheduling as well as the command line interface and routing software.

The Cisco Internetwork Operating System (IOS) may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability.

## DETAILS

Vulnerable Systems:

\* All Cisco products that run Cisco IOS Software.

Cisco IOS may be susceptible to remote code execution through attack vectors such as specific heap-based overflows in which internal operating system timers may execute arbitrary code from portions of memory that have been overwritten via exploitation.

## Securiteam: [NEWS] Cisco IOS Heap-based Overflow Vulnerability

In many cases, a heap-based overflow in Cisco IOS will simply corrupt system memory and trigger a system reload when detected by the "Check Heaps" process, which constantly monitors for such memory corruption. In a successful attack against an appropriate heap-based overflow, it is possible to achieve code execution without the device crashing immediately.

Successful exploitations of heap-based buffer overflow vulnerabilities in Cisco IOS software often result in a Denial of Service because the exploit causes the router to crash and reload due to inconsistencies in running memory. In some cases it is possible to overwrite areas of system memory and execute arbitrary code from those locations. In the event of successful remote code execution, device integrity will have been completely compromised.

For more information visit original article at:

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a008055ef31.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a008055ef31.shtml)  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a008055ef31.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a008055ef31.shtml)

### ADDITIONAL INFORMATION

The original article can be found at:

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a008055ef31.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a008055ef31.shtml)  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a008055ef31.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a008055ef31.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.