



August 22, 2006

---

McAfee, Inc.  
McAfee® Avert® Labs Security Advisory  
Public Release Date: 2006-08-22

## Linux Kernel SCTP Privilege Elevation Vulnerability

CVE-2006-3745

---

- **Synopsis**

The Linux kernel is susceptible to a locally exploitable flaw which may allow local users to gain root privileges and execute arbitrary code at kernel privilege level.

---

- **Vulnerable System or Application**

Linux Kernel Versions: 2.4.23--2.4.32, 2.6 up to and including 2.6.17.7

---

- **Vulnerability Information**

A locally exploitable flaw has been found in the Linux sctp module sctp\_make\_abort\_user function that allows local users to gain root privileges and also execute arbitrary code at kernel privilege level.

---

- **Resolution**

The Linux Kernel Archives has released a fix for this vulnerability. Complete instructions for automatically updating kernel modules can be downloaded at the following site:

<http://www.kernel.org/git/?p=linux/kernel/git/stable/linux-2.6.17.y.git;a=commit;h=96ec9da385cf72c5f775e5f163420ea92e66ded2>

---

- **Credits**

This vulnerability was discovered by Wei Wang of McAfee Avert Labs.

---

- **Legal Notice**

Copyright (C) 2006 McAfee, Inc.

The information contained within this advisory is provided for the convenience of McAfee's customers, and may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way. McAfee makes no representations or warranties regarding the accuracy of the information referenced in this document, or the suitability of that information for your purposes.

McAfee, Inc. and McAfee Avert Labs are registered Trademarks of McAfee, Inc. and/or its affiliated companies in the United States and/or other Countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.