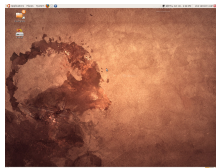


28 November 2008

By: Marius Nestor, Linux Editor



Ubuntu 8.10

[Newly Discovered Kernel Vulnerabilities Affect All Ubuntu Users](#)

[Update now](#)

On November 27th, the Ubuntu developers [announced](#) the availability of a major security update for the following Ubuntu distributions: 6.06 LTS, 7.10, 8.04 LTS and 8.10 (also applies to Kubuntu, Edubuntu and Xubuntu). The update patches nine security issues (see below for details) discovered in the Linux kernel packages. Therefore, it is strongly recommended to update your system as soon as possible!

The following Linux kernel vulnerabilities have been discovered:

1. The Xen hypervisor block driver couldn't accurately validate incoming requests. Therefore, a user with root privileges could crash a system and cause a DoS (Denial of Service) attack by executing malicious I/O requests. This issue affects only Ubuntu 7.10.
2. The i915 video driver couldn't accurately validate memory addresses. Therefore, an attacker could remap memory and cause a system crash, leading to a DoS (Denial of Service) attack. Ubuntu 6.06 LTS, 7.10 and 8.04 LTS users are not affected by this issue. Ubuntu 8.10 users should update their systems to correct this vulnerability!
3. When files were created in the setgid directories, the Linux kernel package couldn't accurately strip permissions. Because of this, a local user could gain extra group privileges. This issue was discovered by David Watson and it affects only Ubuntu 6.06 LTS users!
4. When file splice requests were handled, the Linux kernel package couldn't accurately reject the "append" flag. Therefore, a local attacker could create changes to random locations in a file by bypassing the append mode. This issue was discovered by Olaf Kirch and Miklos Szeredi, and affects only Ubuntu 7.10 and 8.04 LTS users!
5. The SCTP stack couldn't accurately handle INIT-ACK. Because of this, a remote user could send specially crafted SCTP traffic and crash the system, leading to a DoS (Denial of Service) attack. This issue affects only Ubuntu 8.10 users!
6. The SCTP stack couldn't accurately handle the length of bad packets. Because of this, a remote user could send specially crafted SCTP traffic and crash the system, leading to a DoS (Denial of Service) attack. This issue affects only Ubuntu 8.10 users!
7. The HFS+ filesystem had several flaws. Because of this, a user could be tricked to mount a malicious HFS+ filesystem, which could lead to a DoS (Denial of Service) attack and crash the system. This issue was discovered by Eric Sesterhenn, and affects all Ubuntu users!
8. The Unix Socket handler couldn't accurately process the SCM_RIGHTS message. Therefore, a local attacker could create a malicious socket request and crash the system, leading to a DoS (Denial of Service) attack. This issue affects all Ubuntu users!
9. The i2c audio driver couldn't accurately validate several function pointers. Therefore, a local users could obtain root privileges and crash the system, leading to a DoS (Denial of Service) attack. This issue affects all Ubuntu users!

The above Linux kernel vulnerabilities can be fixed if you update your system today to the following specific packages:

- For Ubuntu 6.06 LTS, users should update their kernel packages to linux-image-2.6.15-53.74

- For Ubuntu 7.10, users should update their kernel packages to linux-image-2.6.22-16.60

- For Ubuntu 8.04 LTS, users should update their kernel packages to linux-image-2.6.24-22.45

- For Ubuntu 8.10, users should update their kernel packages to linux-image-2.6.27-9.19

Don't forget to reboot your computer after this update! You can verify the kernel version by typing the `sudo dpkg -l linux-image-2.6.27-9-generic` command in a terminal (the example is for Ubuntu 8.10 users).

ATTENTION: Due to an unavoidable ABI change, the kernel packages have a new version number, which will force you to reinstall or recompile all third-party kernel modules you might have installed. For example, after the upgrade to the above version of your kernel package, a software such as VirtualBox will NOT work anymore, therefore you must recompile its kernel module by issuing a specific command in the terminal. Moreover, if you use the linux-restricted-modules package, you have to update it as well to get modules that work with the new Linux kernel version.

Get the latest version of Ubuntu right now from [Softpedia](#). Don't forget to share it with your friends and family.