

2 July 2009

Ubuntu wallpaper
Aratech Systems

By: Marius Nestor, Linux Editor

[New Kernel Vulnerabilities Affect Ubuntu 6.06, 8.04, 8.10 and 9.04 OSes](#)

All Ubuntu users should update their systems as soon as possible

Earlier today, Canonical has announced the availability of a major security update for the following Ubuntu distributions: 6.06 LTS, 8.04 LTS, 8.10 and 9.04 (also applies to Kubuntu, Edubuntu and Xubuntu). The update patches no more than 15 security issues (see below for details) discovered in the Linux kernel packages by various hackers. Therefore, it is strongly recommended to update your system as soon as possible!

The following Linux kernel vulnerabilities were discovered:

1. When `root_squash` was active, NFS clients could create device nodes. This could lead to loss of privacy. The issue was discovered by Igor Zhbanov, and affects only Ubuntu 8.10 and 9.04 users.
2. SELinux failed to handle various network checks if `compat_net=1` was enabled. Because of this, network checks could be bypassed by a local attacker. The issue was discovered by Dan Carpenter, and affects only Ubuntu 8.10 and 9.04 users.
3. Memory was incorrectly initialized in AGP subsystem, which could lead to loss of privacy. The issue was discovered by Shaohua Li.
4. The VMX implementation of KVM failed to handle various registers. This could lead to a DoS attack and crash the affected system. The issue was discovered by Benjamin Gilbert, and affects only Ubuntu 8.04 LTS, 8.10 and 9.04 users (32-bit versions).
5. The Amateur Radio X.25 Packet Layer Protocol failed to validate various fields, which could lead to loss of privacy. The issue was discovered by Thomas Pollet.
6. NFS failed to handle long filenames. This could lead to a DoS attack and crash the affected system. The issue was discovered by Trond Myklebust, and affects only Ubuntu 6.06 LTS users.
7. The Linux kernel failed to handle `CAP_KILL` and it could lead to a DoS attack. The issue was discovered by Oleg Nesterov.
8. Signal handling was incorrectly limited to process namespaces, which could lead to a DoS attack. The issue was discovered by Daniel Hokka Zakrisson, and affects only Ubuntu 8.04 LTS users.
9. Support for network namespace in IPv6 was incorrectly handled. This could lead to a DoS attack and crash the affected system. The issue was discovered by Pavel Emelyanov, and affects only Ubuntu 8.10 and 9.04 users.
10. The e1000 network driver failed to validate various fields. This could lead to a DoS attack and crash the affected system. The issue was discovered by Neil Horman.
11. CIFS failed to check the lengths when various mount requests were handled. Because

of this, restricted applications could be executed. This could lead to a DoS attack and crash the affected system. The issue was discovered by Pavan Naregundi.

12. NFSv4 failed to handle execute permissions. The issue was discovered by Simon Vallet and Frank Filz.

13. Buffer overflows were discovered in the code of the CIFS client. This could lead to a system crash. The issue was discovered by Jeff Layton and Suresh Jayaraman.

14. On Sparc architecture, the /proc/iomem was incorrectly initialized. This could lead to a DoS attack and crash the affected system. The issue was discovered by Mikulas Patocka, and affects only Ubuntu 8.04 LTS, 8.10 and 9.04 users.

15. OCFS2 failed to handle various splice operations. This could lead to a DoS attack and hang the affected system. The issue was discovered by Miklos Szeredi, and affects only Ubuntu 8.04 LTS, 8.10 and 9.04 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-2.6.15-54.77

- For Ubuntu 8.04 LTS, users should update their kernel packages to linux-image-2.6.24-24.55

- For Ubuntu 8.10, users should update their kernel packages to linux-image-2.6.27-14.35

- For Ubuntu 9.04, users should update their kernel packages to linux-image-2.6.28-13.45

Don't forget to reboot your computer after this update! You can verify the kernel version by typing the `sudo dpkg -l linux-image-2.6.28-13-generic` command in a terminal (the example is for Ubuntu 9.04 users ONLY).

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 piece of 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!