H-Online.com
Several Linux distributors are releasing updated kernel packages to close security holes in the kernel. For instance, very large packets can reportedly be used to remotely provoke a flaw in the TCP/IPv4 stack`s ip_defrag() (net/ipv4/ip_fragment.c) function. This can potentially cause null-pointer dereferencing and crash a system.

Whether the flaw can also be exploited to execute code at kernel level by users that are logged into a system at restricted privilege level, which was the case with several previous null-pointer dereferencing bugs, is not mentioned in the distributors` and kernel developers` descriptions. The flaw was discovered in Linux kernel 2.6.32-rc8 and has been fixed in the final version.

In addition, the new kernel packages fix a vulnerability in the Ext4 file system code. It appears access privileges are not sufficiently checked when the ˝move extents˝ I/O control is called. According to the Ubuntu developers, an attacker (who is logged into a system) can exploit this to overwrite arbitrary data on the system. According to Ubuntu, this can not only cripple a system, but it potentially also allows attackers to specifically manipulate a system in order to obtain root access. The Ext4 file system is installed by default under Ubuntu 9.10, openSUSE 11.2 and Fedora. The commercial Linux systems by Red Hat and Novell, however, still use Ext3 and should be unaffected. Not all the distributors have already released new packages to close the Ext4 hole, but they will probably do so shortly.