

Not long ago, some people discovered a severe security flaw in older linux kernels when handling core dumps.

Vulnerable Systems:

- * Linux Kernel 2.6.17.4 and prior
- * Linux Kernel 2.6.16.24 and prior

The kernel does not check write permissions when writing a core file.

If an attacker can change into a directory where he/she doesn't has write permissions and makes a specially crafted file produce a corefile, the attacker might gain root access.

A know exploit uses `/etc/cron.*` to make a cronjob executed by root. Other attack might be possible, too.

To prevent the exploit above, a `chmod 750 /etc/cron.*` or a `chattr -i /etc/cron.d` might prevent this attack.

Options are that you upgrade to the newest kernel as soon as possible or you change the core file name scheme to a absolute path where normal users don't have read/write/execute permission and no program is doing anything with files in this directory.

This vulnerable is critical, don't delay fixing!

See Also:

- * Securiteam: Linux Kernel 2.6.x PRCTL Core Dump Handling (Exploit)

Support this site