

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)

image:rdf newsfeed / //static.linuxhowtos.org/data/rdf.png (null)

|  
image:rss newsfeed / //static.linuxhowtos.org/data/rss.png (null)

|  
image:Atom newsfeed / //static.linuxhowtos.org/data/atom.png (null)

- Powered by

image:LeopardCMS / //static.linuxhowtos.org/data/leopardcms.png (null)

- Running on

image:Gentoo / //static.linuxhowtos.org/data/gentoo.png (null)

-

Copyright 2004-2020 Sascha Nitsch Unternehmensberatung GmbH

image:Valid XHTML1.1 / //static.linuxhowtos.org/data/xhtml.png (null)

:

image:Valid CSS / //static.linuxhowtos.org/data/css.png (null)

:

image:buttonmaker / //static.linuxhowtos.org/data/buttonmaker.png (null)

- Level Triple-A Conformance to Web Content Accessibility Guidelines 1.0 -

- Copyright and legal notices -

Time to create this page: ms

<!--

image:system status display / /status/output.jpg (null)

-->

bodyloaded();