

Re: [PATCH] x86: introduce /dev/mem restrictions with a config option

Re: [PATCH] x86: introduce /dev/mem restrictions with a config option

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2008-01/msg13353.html>

- *From:* devzero@xxxxxx
 - *Date:* Thu, 31 Jan 2008 15:04:28 +0100
-

nice !

did you think about some boot-time param , e.g. "insecure-devmem" or something like that?

recompiling kernel is time consuming.....

From: Arjan van de Ven <arjan@xxxxxxxxxxxxxxxxxx>
Subject: [PATCH] x86: introduce /dev/mem restrictions with a config option

This patch introduces a restriction on /dev/mem: Only non-memory can be read or written unless the newly introduced config option is set.

The X server needs access to /dev/mem for the PCI space, but it doesn't need access to memory; both the file permissions and SELinux permissions of /dev/mem just make X effectively super-super powerful. With the exception of the BIOS area, there's just no valid app that uses /dev/mem on actual memory. Other popular users of /dev/mem are rootkits and the like. (note: mmap access of memory via /dev/mem was already not allowed since a really long time)

People who want to use /dev/mem for kernel debugging can enable the config option.

The restrictions of this patch have been in the Fedora and RHEL kernels for at least 4 years without any problems.

Signed-off-by: Arjan van de Ven <arjan@xxxxxxxxxxxxxxxxxx>

Jetzt neu! Schützen Sie Ihren PC mit McAfee und WEB.DE. 30 Tage kostenlos testen. <http://www.pc-sicherheit.web.de/startseite/?mc=022220>

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in

Re: [PATCH] x86: introduce /dev/mem restrictions with a config option

Re: [PATCH] x86: introduce /dev/mem restrictions with a config option

the body of a message to majordomo@xxxxxxxxxxxxxxxx

More majordomo info at <http://vger.kernel.org/majordomo-info.html>

Please read the FAQ at <http://www.tux.org/lkml/>