

## [CAN-2005-0204]: AMD64, allows local users to write to privileged IO ports via OUTS instruction

*Source:* <http://linux.derkeiler.com/Mailing-Lists/Kernel/2005-02/6528.html>

---

*From:* micah milano ([micaho\\_at\\_gmail.com](mailto:micaho_at_gmail.com))

*Date:* 02/28/05

Date: Mon, 28 Feb 2005 15:27:13 -0600

To: [linux-kernel@vger.kernel.org](mailto:linux-kernel@vger.kernel.org)

Hello,

CAN-2005-0204 reads:

Linux kernel before 2.6.9, when running on the AMD64 and Intel EM64T architectures, allows local users to write to privileged IO ports via the OUTS instruction.

Although this says "before 2.6.9" this *includes* 2.6.8 (and 2.4.29) as well as 2.6.9 and apparently it includes 2.6.10 and soon to be released 2.6.11 based on my browsing through the changelogs and not seeing a mention of this, or that particular file being changed. I do see that the particular function where this is located has changed slightly, the patch still seems applicable.

Kernel 2.4.29 appears to have a similar vulnerability, although this patch would not apply cleanly to that tree, but looks relatively trivial to modify appropriately.

Apparently this hole has not migrated upstream somehow and so I am posting this message to find out where its at.

REDHAT:RHSA-2005:092

URL:<http://www.redhat.com/support/errata/RHSA-2005-092.html>

The RedHat bug associated with this is located at:

[https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=148855](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=148855)

A patch to fix the problem is located here (also linked to the RedHat bug):

<https://bugzilla.redhat.com/bugzilla/attachment.cgi?id=110424&action=view>

This apparently only affects AMD64 and EM64T.

Thanks,  
micah

Linux-Kernel: [CAN-2005-0204]: AMD64, allows local users to write to privileged IO ports via OUTS instruction

—

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to [majordomo@vger.kernel.org](mailto:majordomo@vger.kernel.org)

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

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