Re: Catching NForce2 lockup with NMI watchdog

Source: http://linux.derkeiler.com/Mailing−Lists/Kernel/2003−12/2940.html

---

From: Maciej W. Rozycki (*macro_at_ds2.pg.gda.pl*)
Date: 12/12/03

```
Date:   Fri, 12 Dec 2003 18:21:16 +0100 (CET)
To: "Richard B. Johnson" <root@chaos.analogic.com>
```

On Fri, 12 Dec 2003, Richard B. Johnson wrote:

> > Sometimes the NMI watchdog works in principle, but its activation leads
> > to system instability −− almost always this is a symptom of buggy SMM code
> ^^^
> > executed by the BIOS behind our back (NMIs are disabled by default in the
> ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
> > SMM, but careless code may enable them by accident).
>
> The NMI vector goes to Linux code. In fact all interrupt vectors
> go to Linux code. There is no way that some BIOS code could possibly
> be accidentally executed here. Some Linux code would have to
> call some 16−bit BIOS code somewhere, and it doesn't even know
> where..........

The problem happens when the SMM is active (i.e. the BIOS code is being executed) after an SMI has been received during Linux operation (SMIs may get triggered due to various reasons −− a parity/ECC error caught by the chipset, an access to an emulated 8042 controller, a power failure in a notebook, etc.) and an NMI arrives. When in the SMM, no interrupt (including the NMI) causes a switch back into the protected mode (and the processor expects real−mode style interrupt vectors), so the Linux's NMI handler is never reached and the SMM's NMI handler (if at all initialized) isn't appropriate for handling the NMI watchdog. Since the SMM cannot know what NMIs are used for in a particular OS, the code should best keep NMIs disabled −− then an arriving NMI event is latched and postponed until after the RSM instruction is executed.

The SMM was invented to be transparent to a running OS, but care has to be taken for this to be true and firmware bugs sometimes make the SMM activity visible.

```
−−
+  Maciej W. Rozycki, Technical University of Gdansk, Poland   +
+−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−+
+        e−mail: macro@ds2.pg.gda.pl, PGP key available       +
−
```