Subject: SecurityFocus Article
Posted by Ed White on Thu, 11 May 2006 14:51:41 GMT
View Forum Message <> Reply to Message

A researcher of the french NSA discovered a scary vulnerability in modern x86 cpus and chipsets that expose the kernel to direct tampering.

The problem is that a feature called System Management Mode could be used to bypass the kernel and execute code at the highest level possible: ring zero.

The big problem is that the attack is possible thanks to the way X Windows is designed, and so the only way to eradicate it is to redesign it, moving video card driver into the kernel, but it seems that this cannot be done also for missing drivers and documentation!

I would like to know if OpenVZ barriers could be bypassed using this attack, or not. Maybe we will need a patch for the kernel, or for OpenVZ itself, or what?

Any hint is appreciated.

The quest for ring 0

by Federico Biancuzzi
2006-05-10

Federico Biancuzzi interviews French researcher Loïc Duflot to learn about the System Management Mode attack, how to mitigate it, what hardware is vulnerable, and why we should be concerned with recent X Server bugs.
http://www.securityfocus.com/columnists/402