Published on *Tux Machines* (http://www.tuxmachines.org)

Device drivers filled with flaws

By *srlinuxx*
Created *27/05/2005 - 3:56pm*
Submitted by srlinuxx on Friday 27th of May 2005 03:56:44 PM Filed under Security [1]

Operating system vendors and hardware makers should commit more resources toward systematically auditing Windows and Linux device-driver code for flaws, security researchers say.

While buffer overflows, a type of memory flaw that can lead to serious vulnerabilities, are quickly being eradicated in critical applications, the flaws are still easily found in device drivers, said David Maynor, a research engineer for Internet Security Systems' X-Force vulnerability analysis group.

"If you look through the device driver code, there are a lot of problems," he said in a recent interview. "The state of the code's security is not strong." During a few hours on a recent plane flight, for example, Maynor found more than a dozen glitches in several Windows XP drivers.

Windows is not the only operating system at risk. A survey of the Linux 2.6.9 kernel code performed by automated-code-checking software maker Coverity found that, while the overall quality of the code had increased significantly, more than 50 percent of flaws appeared in device drivers. Many of those flaws may not affect system security, but the ratio is generally indicative of the quality of the code, said Seth Hallem, CEO of Coverity.

"The people writing the device drivers are not generally the core programmers," he said. "It is not the operating-system implementers themselves -- the Linux programmers or Windows developers -- it is generally the vendors."

The warnings come as operating-system developers have placed security higher on their to-do lists. While the Windows and Linux operating systems have both undergone significant audits in the past several years, many device drivers -- especially those created by third-party hardware providers -- have seemingly escaped rigorous testing.

Device driver flaws can be more dangerous than other application vulnerabilities because device drivers are, in most cases, part of the kernel itself and subverting the critical software gives an attacker direct access to the kernel. Moreover, drivers that have direct memory access (DMA) -- such as USB drivers, CardBus drivers, graphics drivers and sound drivers -- could be used to overwrite system memory and exploit the system.

"Since drivers run in kernel-privilege state, if you can take them over you are in a privileged position," said Bill Weinberg, Linux evangelist for the Open Source Development Labs. "But it is not an trivial thing, you are more likely to crash the system."

"You no longer have a single computer," he said. "It is a collection of subsystems and device drivers are becoming that much more important."

Full Article [2].

Security

Source URL: http://www.tuxmachines.org/node/1094

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://www.securityfocus.com/news/11260