

Learn from 'Month of Kernel Bugs'

Rich Mogull

The Month of Kernel Bugs is a serious wake-up call about the vulnerability of the most fundamental element of the operating system. Begin preparing now for more, and more damaging, attacks against the OS kernel.

NEWS ANALYSIS

Event

On 1 November 2006, independent security researchers launched a campaign called the Month of Kernel Bugs that targets flaws in operating system (OS) kernels. The researchers plan to release one new exploit targeting an unpatched flaw in an OS kernel each day of November. The first exploits released target Apple PowerBook wireless drivers; others target other OSs, including Linux and Windows. More details are available at <http://kernel.fun.blogspot.com>.

Analysis

The Month of Kernel Bugs highlights the poorly understood but growing threat of flaws in the kernel — the most fundamental part of any OS. The kernel is typically hardened, and therefore better-protected than other software elements; it is also technically more challenging to leverage a damaging attack in the kernel, because many user-based OS functions are located at a higher level. However, because anything running in the kernel is completely trusted, an attacker with the necessary skills can take full control of the exploited system from the kernel. The most common vectors for kernel attacks are flaws in file systems and device drivers.

The Month of Kernel Bugs was inspired by a recent advance in the security research community: the free availability of "fuzzing" tools. Fuzzing is an automated software testing process that uses a tool to rapidly create randomly generated, often malformed input data until the process being tested crashes; these tools are particularly effective in discovering software vulnerabilities in device drivers and file systems. A second advance, the incorporation of kernel exploits into the free Metasploit penetration testing tool, is a very early indication that the complex exploitation of kernel flaws will be simplified in the future. Metasploit significantly reduces the skill level required to launch remote security exploits, in some cases eliminating the complexity of working directly in the kernel. Metasploit's kernel module (currently under development for the Windows OS only) will focus on leveraging remote kernel exploits, predominantly local wireless attacks.

These twin developments will help to automate the vulnerability discovery process and simplify the exploit process for a subset of these vulnerabilities. Most of the vulnerabilities revealed in the Month of Kernel Flaws are expected to focus on Unix-based local vulnerabilities and cross-platform wireless flaws. All parties with a stake in OS integrity — including hardware and software vendors and enterprises using the affected OSs — should take the Month of Kernel Bugs as a serious wake-up call about the vulnerability of the OS kernel.

RECOMMENDATIONS

- **Hardware and software vendors:** Move immediately to improve the testing of software, especially device drivers and operating system code, using "fuzzing" techniques.
- **Enterprises:** Add device driver configuration and patching to your vulnerability management processes, but remember that even among computers using the same hardware version, internal devices — and therefore drivers — may vary.

RECOMMENDED READING

- "Manage Device Driver Vulnerabilities on Macs or PCs Quickly" — Enterprises need to plug a device-driver exploit before valuable information is lost or compromised. **By Rich Mogull**

- "Patch Management Best Practices" — Patch management best practices operationalize the steps of the vulnerability management life cycle. **By Mark Nicolett and Ronni Colville**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509