

**The Register**  
Biting the hand that feeds IT

**On-demand Webcast**

**Application Security RegCast**  
Jump start your Application Security initiatives with practical advice and guidance from The Register's expert panel

**Click here to watch**

Original URL: [http://www.theregister.co.uk/2009/08/14/critical\\_linux\\_bug/](http://www.theregister.co.uk/2009/08/14/critical_linux_bug/)

## Bug exposes eight years of Linux kernel

### Passes it's-not-crying-wolf test

By [Dan Goodin in San Francisco](#)

Posted in [Security](#), 14th August 2009 00:54 GMT

[Free whitepaper – Avoiding 7 common mistakes of IT security compliance](#)

Linux developers have issued a critical update for the open-source OS after researchers uncovered a vulnerability in its kernel that puts most versions built in the past eight years at risk of complete takeover.

The bug involves the way kernel-level routines such as `sock_sendpage` react when they are left unimplemented. Instead of linking to a corresponding placeholder, (for example, `sock_no_accept`), the function pointer is left uninitialized. `sock_sendpage` doesn't always validate the pointer before dereferencing it, leaving the OS open to local privilege escalation that can completely compromise the underlying machine.



"Since it leads to the kernel executing code at NULL, the vulnerability is as trivial as it can get to exploit," security researcher Julien Tinnes [writes here](http://blog.cr0.org/2009/08/linux-null-pointer-dereference-due-to.html) (<http://blog.cr0.org/2009/08/linux-null-pointer-dereference-due-to.html>). "An attacker can just put code in the first page that will get executed with kernel privileges."

Tinnes and fellow researcher Tavis Ormandy released proof-of-concept code that they said took just a few minutes to adapt from a previous exploit they had. They said all 2.4 and 2.6 version since May 2001 are affected.

Security researchers not involved in the discovery were still studying the advisory at time of writing, but at least one of them said it appeared at first blush to warrant an immediate action.

"This passes my it's-not-crying-wolf test so far," said Rodney Thayer, CTO of security research firm Secorix. "If I had some kind of enterprise-class Linux system like a Red Hat Enterprise Linux...I would really go check and see if this looked like it related, and if my vendor was on top of it and did I need to get a kernel patch."

This is the second time in less than a month that a serious security vulnerability has been reported in the Linux kernel. In mid July, a researcher alerted Linux developers to a separate "[NULL pointer dereference](http://www.theregister.co.uk/2009/07/17/linux_kernel_exploit/)" bug that put newer versions at risk of complete compromise. The bug, which was located in several parts of the kernel, attracted plenty of notice because it bit even when SELinux, or Security-Enhanced Linux, implementations were running.

More about the latest vulnerability is [here](http://archives.neohapsis.com/archives/fulldisclosure/2009-08/0174.html), and additional details about the patch are [here](http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=e694958388c50148389b0e9b9e9e8945cf0f1b98). ®

## Related stories

[Sequoia e-voting machine commandeered by clever attack](http://www.theregister.co.uk/2009/08/12/sequoia_evoting_machine_felled/) (12 August 2009)

[http://www.theregister.co.uk/2009/08/12/sequoia\\_evoting\\_machine\\_felled/](http://www.theregister.co.uk/2009/08/12/sequoia_evoting_machine_felled/)

[Clever attack exploits fully-patched Linux kernel](http://www.theregister.co.uk/2009/07/17/linux_kernel_exploit/) (17 July 2009)

[http://www.theregister.co.uk/2009/07/17/linux\\_kernel\\_exploit/](http://www.theregister.co.uk/2009/07/17/linux_kernel_exploit/)

[Google Oompa-Loompas dream of virus-free OS](http://www.theregister.co.uk/2009/07/09/google_chrome_os_security/) (9 July 2009)

[http://www.theregister.co.uk/2009/07/09/google\\_chrome\\_os\\_security/](http://www.theregister.co.uk/2009/07/09/google_chrome_os_security/)

[Microsoft fortifies Windows 7 kernel with overrun buster](http://www.theregister.co.uk/2009/05/28/windows_kernel_safe_unlinking/) (28 May 2009)

[http://www.theregister.co.uk/2009/05/28/windows\\_kernel\\_safe\\_unlinking/](http://www.theregister.co.uk/2009/05/28/windows_kernel_safe_unlinking/)

[Canonical punts Ubuntu Jaunty Jackalope](http://www.theregister.co.uk/2009/04/20/ubuntu_9_04_released/) (20 April 2009)

[http://www.theregister.co.uk/2009/04/20/ubuntu\\_9\\_04\\_released/](http://www.theregister.co.uk/2009/04/20/ubuntu_9_04_released/)

[Mac and Linux Bastilles assaulted by new attacks](http://www.theregister.co.uk/2009/04/16/alternative_os_flaws/) (16 April 2009)

[http://www.theregister.co.uk/2009/04/16/alternative\\_os\\_flaws/](http://www.theregister.co.uk/2009/04/16/alternative_os_flaws/)

[Researchers poke holes in Intel's anti-tampering tech](http://www.theregister.co.uk/2009/01/07/intel_vpro_hack/) (7 January 2009)

[http://www.theregister.co.uk/2009/01/07/intel\\_vpro\\_hack/](http://www.theregister.co.uk/2009/01/07/intel_vpro_hack/)

[Red Hat extends RHEL release support](http://www.theregister.co.uk/2008/12/18/rhel_extended_release_support/) (18 December 2008)

[http://www.theregister.co.uk/2008/12/18/rhel\\_extended\\_release\\_support/](http://www.theregister.co.uk/2008/12/18/rhel_extended_release_support/)

© Copyright 1998–2009