

[VulnWatch] Addendum, recent Linux <= 2.4.27 vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-11/0007.html>

From: Paul Starzetz (*ihaquer_at_isec.pl*)

Date: 11/19/04

Date: Fri, 19 Nov 2004 20:26:21 +0100 (CET)

To: bugtraq@securityfocus.com, <full-disclosure@lists.netsys.com>, <vulnwatch@vulnwatch.org>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hi,

while looking at the changelog for 2.4.28, I've found, that a bug I independently came over some days ago has been fixed in that release:

David S. Miller:

- o [AF_UNIX]: Serialize dgram read using semaphore just like stream

That fixes missing serialization in `unix_dgram_recvmsg()`.

I was slightly suprised reading the 2.4.27 code and I strongly believe that the flaw is fully exploitable to gain elevated privileges.

There is a subtle race condition finally permitting a non-root user to increment (up to 256 times) any arbitrary location(s) in kernel space.

The condition is not easy to exploit since an attacker must trick `kmalloc()` to sleep on allocation of a special chunk of memory and then convince the scheduler to execute another thread. But it is feasible.

Conclusion: update as quick as possible to 2.4.28.

Paul Starzetz

iSEC Security Research

<http://isec.pl/>

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.7 (GNU/Linux)

iD8DBQFBnkjiC+8U3Z5wpu4RAiCJAKCpqAD3jD/Ih6CSVxOUW0wnkXVY8QCgs584
x03r/RbphAViQPJrM8Fqj28=

VulnWatch: [VulnWatch] Addendum, recent Linux <= 2.4.27 vulnerabilities

=Adi4

-----END PGP SIGNATURE-----