

Re: FreeBSD-SA-04:13.linux in the wild

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-08/0022.html>

From: Ryan Thompson (ryan_at_sasknow.com)

Date: 08/11/04

Date: Wed, 11 Aug 2004 15:32:12 -0600 (CST)
To: "Gustavo A. Baratto" <gbaratto@superb.net>

Gustavo A. Baratto wrote to Ryan Thompson and freebsd-security@freebsd.org:

> *I think I may have seen such thing before as well... not a freebsd problem*
> *though... It's php's own fault.*
> *php comes with url_fopen enabled by default, so if someone write a*
> *script.php with something like:*
> *include ("\$var");*
>
> *[...]*
>
> *just disabling url_fopen in php.ini would prevent that.*
>
> *If this is not what you have seen, please, I'd like to know more about it.*

Yep, that's almost exactly what happened. The PHP injection by itself is fairly pedestrian, and happens on a fairly regular basis (so we have audits for a whole host of things like this). I just mentioned it to give a bit of background to the attack.

The linux exploit, though, I hadn't spotted in the wild yet, thus my post, here.

– Ryan

--

Ryan Thompson <ryan@sasknow.com>
SaskNow Technologies - <http://www.sasknow.com>
901-1st Avenue North - Saskatoon, SK - S7K 1Y4
Tel: 306-664-3600 Fax: 306-244-7037 Saskatoon
Toll-Free: 877-727-5669 (877-SASKNOW) North America

freebsd-security@freebsd.org mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-security>
To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"