

Re: Report of collision-generation with MD5

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-08/0077.html>

From: Peter Jeremy (*PeterJeremy_at_optushome.com.au*)

Date: 08/26/04

Date: Thu, 26 Aug 2004 18:08:11 +1000
To: Brooks Davis <brooks@one-eyed-alien.net>

On Wed, 2004-Aug-25 13:16:40 -0700, Brooks Davis wrote:

>On Wed, Aug 25, 2004 at 09:51:50PM +0200, *guy@device.dyndns.org* wrote:
>> *I _believe_ answer is "no", because i _think_ the FreeBSD ports system also*
>> *verify the size of the archive(s) (cat /usr/ports/any/any/distinfo to see*
>> *what made me think that).*

I don't believe the size adds much security.

>*Paranoia might suggest adding support for multiple hashes which would*
>*vastly increase the difficulty of finding a collision*

I'd agree with this. Identifying suitable hashes is a more difficult task.

>*Hmm, one thing to think about might be making sure the various archive*
>*formats are hard to pad with junk. I think the stream based ones need*
>*to allow zero padding at the end to support tapes, but it would be*
>*intresting to see if other junk can end up in padding sections without*
>*the archiver noticing. If so, that would be a good thing to find a way*
>*to detect.*

tar uses one (or two) blocks of NULs to mark logical EOF – anything beyond that is ignored. gzip ignores (but warns) about padding after its expected EOF. I'm not sure about bzip2. I suspect it would be possible to include arbitrary padding inside a ZIP file, though probably not at the end. This would make it relatively easy to pad a trojan'd file to any desired size.

--
Peter Jeremy

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"