

Re: MD5 Collisions...

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2007-12/msg00018.html>

- *From:* Eygene Ryabinkin <rea-fbsd@xxxxxxxxxxx>
 - *Date:* Tue, 4 Dec 2007 19:43:45 +0300
-

Josh, good day.

Tue, Dec 04, 2007 at 10:10:32AM -0600, Josh Paetzel wrote:

The usefulness of this with application to the ports collection is questionable, since you should make two colliding archives and both of them should be unpackable and the second should do some evil things. But strictly speaking, there are attacks producing files with the same size and MD5 hash.

<http://www.cits.rub.de/MD5Collisions/> is also a good reading.

It's not really questionable....for all practical purposes it's worthless. In order to generate meaningful same-length collisions you need control of the original file. (Your links go to lengths to explain this...) In the case of a ports distfile if you have control of the original file you really don't need to go to great lengths to generate collisions, you can simply toss your malicious content in there right from the get go.

Yes, thanks for clarifying the point that one should be able to control both sequences in order to produce colliding files with the same size.

But there is at least one scenario, when such attack is useful, if one will be able to produce two colliding source archives. Suppose, I am providing a port with new sources (either the new port or an update to the current one) and I am controlling the source tarballs. The sources will be supposedly reviewed by some parties and they will find no backdoors in it. So the port comes in the systems and it is thought to be good and useful.

Once the port proved itself, I am replacing the good source tarballs with the evil ones (remember, I had prepared two colliding archives) and no one will notice the difference with MD5 + size check. But new port installations will be doing something different from the sources that were reviewed.

Again, this is only theoretical thing with many preconditions, but

Re: MD5 Collisions...

if I am able to make two colliding archives, then other things are not very hard to achieve. People are producing colliding X.509 certificates, so we have an example of not 'just junk colliding content', but something meaningful.

I am not going to flame about the real possibility of doing these for many reasons, and the first one that it is no longer doable for the current ports where SHA256 is in the game. All I wanted to say that there are scenarios where one can exploit MD5 weakness, providing one can extend MD5 collision attacks to archives.

Shutting up.

--

Eygene

freebsd-security@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@xxxxxxxxxxx"