

## Re: Report of collision-generation with MD5

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-08/0055.html>

---

**From:** Peter C. Lai ([sirmoo\\_at\\_cowbert.net](mailto:sirmoo_at_cowbert.net))

**Date:** 08/18/04

Date: Wed, 18 Aug 2004 13:58:04 -0400

To: David Wolfskill <[david@catwhisker.org](mailto:david@catwhisker.org)>

Well while collisions are cryptographically significant, they don't necessarily impact any operational security of the the hash. (Since the collision merely means that there are possibly two inputs which will hash to the same digest). Where this could theoretically mean that someone could alter a signed message, we have to look at the chance that what was intended to be altered will satisfy the conditions for the collision. The only 'real' worry about this issue is that if MD5 is already cryptographically challenged in this manner, it may be more possible to find a way to reverse the hash.

You can read the discussion here:

[http://www.rtfm.com/movabletype/archives/2004\\_08.html#001053](http://www.rtfm.com/movabletype/archives/2004_08.html#001053)

[http://www.rtfm.com/movabletype/archives/2004\\_03.html#000820](http://www.rtfm.com/movabletype/archives/2004_03.html#000820)

On Wed, Aug 18, 2004 at 10:24:27AM -0700, David Wolfskill wrote:

> *Just got a pointer to this via ACM "TechNews Alert" for today:*

>

> <http://www.acm.org/technews/articles/2004-6/0818w.html#item2>

>

> *Seems that "... French computer scientist Antoine Joux reported on*

> *Aug. 12 his discovery of a flaw in the MD5 algorithm, which is often*

> *used with digital signatures...."*

>

> *There's more in the article cited above.*

>

> *Peace,*

> *david*

> --

> *David H. Wolfskill [david@catwhisker.org](mailto:david@catwhisker.org)*

> *Evidence of curmudgeonliness: becoming irritated with the usage of the*

> *word "speed" in contexts referring to quantification of network*

> *performance, as opposed to "bandwidth" or "latency."*

>

> [freebsd-security@freebsd.org](mailto: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"*

--

Peter C. Lai

## FreeBSD-Security: Re: Report of collision-generation with MD5

University of Connecticut  
Dept. of Molecular and Cell Biology  
Yale University School of Medicine  
SenseLab | Research Assistant  
<http://cowbert.2y.net/>

---

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"