SECURITY

MD5 Weaknesses Could Lead to Certificate Forgery

Johnathan Nightingale | December 30, 2008 | 19 responses

Issue

Researchers have recently found weaknesses in the MD5 hash algorithm, relied on by some SSL certificates. Using these weaknesses, an attacker could obtain fraudulent SSL certificates for websites they don't legitimately control.

Impact to users

If a user visits an SSL site presenting a fraudulent certificate, there will be no obvious sign of a problem and the connection will appear to be secure. This could result in the user disclosing personal information to the site, believing it to be legitimate. We advise users to exercise caution when interacting with sites that require sensitive information, particularly when using public internet connections.

Status

This is not an attack on a Mozilla product, but we are nevertheless working with affected certificate authorities to ensure that their issuing processes are updated to prevent this threat. Mozilla is not aware of any instances of this attack occurring in the wild.

Microsoft has released their own advisory as well.

Credit

Alexander Sotirov, Marc Stevens, and Jacob Appelbaum presented this work at the 25th Chaos Communication Congress.

Human Shield

previous article

The Importance of Good Metrics

December 15, 2008

next article

Beware the Security Metric

March 6, 2009

More articles in “Security”

Firefox Security Response to pwn2own 2025

May 17, 2025

Updated GPG key for signing Firefox Releases

April 1, 2025

Enhancing CA Practices: Key Updates in Mozilla Root Store Policy, v3.0

March 12, 2025

Behind the Scenes: Fixing an In-the-Wild Firefox Exploit

October 11, 2024

Firefox will upgrade more Mixed Content in Version 127

June 5, 2024

Recent articles

May 17, 2025

Updated GPG key for signing Firefox Releases

April 1, 2025

Enhancing CA Practices: Key Updates in Mozilla Root Store Policy, v3.0

March 12, 2025

Behind the Scenes: Fixing an In-the-Wild Firefox Exploit

October 11, 2024

Firefox will upgrade more Mixed Content in Version 127

June 5, 2024

19 comments on “MD5 Weaknesses Could Lead to Certificate Forgery”

Phil wrote on December 30, 2008 at 9:09 am:

The research paper is here:

http://www.win.tue.nl/hashclash/rogue-ca/

More details at
http://events.ccc.de/congress/2008/Fahrplan/attachments/1251_md5-collisions-1.0.pdf

---

Robert C. Sheets wrote on December 30, 2008 at 3:17 pm:

Is it possible from the Firefox UI to tell if the certificate for the site I'm visiting is signed using only an MD5 hash, or if there is a certificate in the chain of trust that is signed using only MD5?

Please correct me if I'm wrong, but it seems to me that if all the certificates in the chain use SHA-1 instead of (or in addition to) MD5, it would be possible to prove that an SSL connection is not being attacked in this way. Instructions on how to check this could be helpful for those users who choose to be extra vigilant.

Michael wrote on December 30, 2008 at 6:08 pm:

Download links for a video from the presentation:

http://events.ccc.de/congress/2008/wiki/Streaming#Real_Time_Recordings

---

Sitaram wrote on December 31, 2008 at 12:19 am:

Wouldn't it suffice to set all about:config keys containing md5 to false?

On my setup the only one that was still true was security.ssl3.rsa_rc4_128_md5 and I just set it to false. I figure I'll worry about it if some site I *really* want breaks, until then this is better.

S Miller wrote on December 31, 2008 at 6:48 am:

How difficult would it be for someone to code an add-in to detect an MD5 certificate in use, implemented as a flag or (possibly a canary if that is easier coding)? I am not a Mozilla development-type, and I tried messing about with sqlite3.exe from the command line to try to produce a local list of MD5 certificates from the cert8.db database with no success. I would very much like to have a way to alert my users of a potentially forged SSL site in the event that this vulnerability becomes prevalent in the wild before it is addressed effectively.

-S

wombat wrote on December 31, 2008 at 7:34 am:

This is not a recently discovered weakness in MD5: it was discovered in 2001-2005 and much has been published about it since then. These same researchers already published SSL (X.509) certificates with distinct names on them, but identical MD5 hashes in 2006 – http://www.win.tue.nl/hashclash/TargetCollidingCertificates/. That publication also made the international press at the time.

That Mozilla's products still accept MD5 hashes for secure signing purposes is a bug that can only be explained by ignorance or apathy. This is one of those moments where you say "sorry" and not try to redirect responsibility to others.

There is a clear problem with Mozilla products: the software should be fixed and stop accepting any SSL certificate that uses MD5 checksums altogether (anywhere in the validation chain). After fixing that, you should think hard about out why you didn't do this before.

John wrote on December 31, 2008 at 9:42 am:

Mozilla should have the ability to reject MD5-signed certs or at least alert the user. If there's already such a control, where is it?

Nick Mathewson wrote on December 31, 2008 at 9:55 am:

Can nothing more be done? I'd think that we'd be moving towards rejecting any cert chain with an MD5-based cert in it. I know we don't want to break 30% of the web _now_, but it seems very fragile to leave all users everywhere vulnerable to MITM attacks so long as some CA somewhere has been issuing MD5-based certs.

Gary Covington wrote on December 31, 2008 at 9:30 pm:

How do I as a user tell if the certificate is MD5 or later? The little "locked padlock" symbol doesn't say.

Steven wrote on January 1, 2009 at 6:11 am:

Firefox can patch this vulnerability very quickly and very easily (show the world how quickly a Firefox can mitigate the issue!) using the existing SSL verification mechanisms for example: (xxx website uses an insecure security certificate. The certificate is not trusted because the issuer certificate uses the insecure MD5 algorithm. Error code: sec_error_insecure_MD5_issuer_certificate))

Users can still add an exception to the Rule if needed but it would Mitigate the issue because the user would still be warned…It would also put more pressure on affected websites still using MD5 certificates to update them immediately and further mitigate any attack scenarios…

The amount of websites using MD5 based certificates are small and if they see their certificate not working with Firefox or showing the "Secure Connection Failed" Page they will request a new certificate immediately…

The longer Browsers accept MD5 based certificates the longer it will take to force website operators to update as some people just wouldn't care unless their certificate no longer works…

Kasper wrote on January 1, 2009 at 3:11 pm:

I came here hoping to find an official answer to whether setting the security.ssl3.rsa_rc4_128_md5 option to false is sufficient to protect yourself against this weakness.

Tom K wrote on January 4, 2009 at 12:26 pm:

How about steps to check whether a cert in the chain uses MD5? An advisory concerning Moz. Products like firefox would be nice! Firefox extension that warns when an https connection relying on a MD5 hashed cert is established?

Please take some real steps instead of only copy and pasting the link here. The advice “have caution” is really laughable, how shall i know what to look for if you don’t tell me?

David Mentré wrote on January 15, 2009 at 3:31 am:

Hello,

This security issue shows that the security model of Firefox relying exclusively on third party authentication (i.e. the recent demise of self-signed certificates in Firefox 3) is fundamentally broken.

One should not be more confident in a Verisign certificate than in a self-signed one. What is really meaningful is when something “strange” happens in the background, e.g. when a website changes its certificate (self-signed or not).

Sincerely yours,
David Mentré

---

pakman wrote on January 18, 2009 at 9:16 am:

Breaking SSL, PDP-8's & UltraCapacitors episode 177

a security podcast

download

http://media.grc.com/sn/sn-177-lq.mp3

Johnathan Nightingale wrote on January 21, 2009 at 12:31 pm:

@Nick, and others asking similar questions:

We certainly can look at retiring MD5 as a supported algorithm, in fact that discussion is already happening in the mozilla.dev.tech.crypto newsgroup, and the bugs are being worked on. As you anticipate, the decision will need to take into account how much of the internet it breaks. I've got a related post up about how to answer some of those questions, here:

http://blog.johnath.com/2009/01/21/ssl-information-wants-to-be-free/

Wanda R wrote on January 22, 2009 at 7:42 pm:

I'm not an IT person, just a regular user. I recently switched to Firefox which is quicker and sleeker. Now, all day today, when I try to enter the Facebook application, I get the following…Secure Connection Failed.

An error occurred during a connection to login.facebook.com.

Can't connect securely because the SSL protocol has been disabled.

(Error code: ssl_error_ssl_disabled)

The page you are trying to view can not be shown because the authenticity of the received data could not be verified.

* Please contact the web site owners to inform them of this problem.

event security wrote on January 25, 2009 at 6:52 pm:

@Wanda: I think that was just an intermittent error with Facebook that should have resolved itself.

WEB Consultant wrote on January 25, 2009 at 11:34 pm:

MD5 hash algorithm is very old. I think security specialists have to develop something more usefull and strong.