

MD5 Considered Harmful Today: Creating a rogue CA certificate

2009-01-06 / 2009-01-07

Credit: **Alexander Sotirov** (<https://cxsecurity.com/author/Alexander+Sotirov/1/>)

Risk: **Medium**

Local: **No**

Remote: **Yes**

CVE: **CVE-2004-2761**
(<https://cxsecurity.com/cveshow/CVE-2004-2761/>)

CWE: **CWE-310**
(<https://cxsecurity.com/cwe/CWE-310/>)

CVSS Base Score: **5/10**
Exploitability Subscore: **10/10**
Attack complexity: **Low**
Confidentiality impact: **None**
Availability impact: **None**

Impact Subscore: **2.9/10**
Exploit range: **Remote**
Authentication: **No required**
Integrity impact: **Partial**

Our research team, consisting of 7 researchers from the United States, Switzerland and the Netherlands, was able to execute a practical MD5 collision attack and create a rogue Certification Authority trusted by all common web browsers. This allows us to perform transparent man-in-the-middle attacks against SSL connections and monitor or tamper with the traffic to secure websites or email servers.

The infrastructure of Certification Authorities is meant to prevent exactly this type of attack. Our work shows that known weaknesses in the MD5 hash function can be exploited in realistic attack, due to the fact that

t even after years of warnings about the lack of security of MD5, some root CAs are still using this broken hash function.

More details:

<http://www.phreedom.org/research/rogue-ca/>

Enjoy!

Alex

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.9 (Darwin)

iEYEAARECAAYFAk1aUXEACgkQ6MVeVwnnQQStoQCdF5eIqxKx515soMee2sVgEACc
N7AAAn1g0tnDC5f1tqB/RxMpfZ1rY+wnU
=Fpsd

-----END PGP SIGNATURE-----

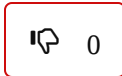
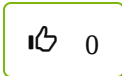
References:

- https://blogs.verisign.com/ssl-blog/2008/12/on_md5_vulnerabilities_and_mit.php
- <http://www.win.tue.nl/hashclash/SoftIntCodeSign/>
- <http://www.win.tue.nl/hashclash/rogue-ca/>
- <http://www.securityfocus.com/bid/33065>
- <http://www.securityfocus.com/archive/1/archive/1/499685/100/0/threaded>
- <http://www.phreedom.org/research/rogue-ca/>
- <http://www.microsoft.com/technet/security/advisory/961509.mspx>
- http://www.doxpara.com/research/md5/md5_someday.pdf
- <http://blogs.technet.com/swi/archive/2008/12/30/information-regarding-md5-collisions-problem.aspx>
- <http://blog.mozilla.com/security/2008/12/30/md5-weaknesses-could-lead-to-certificate-forgery/>

See this note in RAW Version (<https://cxsecurity.com/ascii/WLB-2009010122>)

Post

Vote for this issue:



50%

50%

Comment it here.

Nick (*)

Email (*)

Video

Text (*)

Copyright 2026, cxsecurity.com