Bruce Schneier blogjára 2015. október 8-án került fel a Marc Stevens vezette csapat tanulmánya az első teljes (80 körös) SHA-1 ütközésről. Az "első teljes" jelző csak annyiból igaz, hogy korábban a "Malicious SHA-1" csapat tagjai már tudtak módosított konstans értékekkel 80 körös ciklus végére ütközést produkálni, a mostani esetnél a konstansok ugyan már szabványosak, de az IV értékét még módosítani kellett (a szabványos Initialization Vector: H0..H4 az IETF RFC 3174 dokumentumban található). Ettől függetlenül ez nagy eredmény és bár Bruce bácsi azt mondja, hogy "don't panic", emlékszünk rá, hogy az MD5-nél is ugyanígy kezdődött a haláltusa, ezért ő is hozzáteszi, hogy "but prepare for a future panic".

Mennyire volt nehéz ilyen ütközést létrehozni? A kutatók azt állítják, hogy "only 10 days of computation on a 64 GPU cluster were necessary to perform the attack". Ha HW-közelibb eszközöket (FPGA vagy ASIC) használtak volna, akkor lehet, hogy még ennél is hamarabb sikerül nekik... A megadott test vector adatai mindenesetre jók: a két különböző üzenet esetén valóban létrehozható ugyanaz az SHA-1 lenyomat érték (80. kör végén, de módosított IV-vel).

Vajon mennyire fogja ez az eredmény befolyásolni az SHA-1 algoritmuson alapuló kulcsok elfogadását? Bár, a Microsoft is közzétett korábban figyelmeztetést, hogy a hitelesítés-szolgáltatók ne használják már az újonnan kiadott végfelhasználói tanúsítványoknál (code signing és SSL/TLS web server eseteket említ csak) az SHA-1 algoritmust, mert ezeket nem fogja tudni érvényesnek találni 2016. január 1. után, azonban a CA tanúsítványok esetleges visszavonására még nem utal a bejegyzés. Pedig annak idején, amikor a Flame megmutatta, hogy mekkora problémát lehet okozni azzal, hogy MD5 ütközés révén, egy MD5-RSA aláírással ellátott code signing tanúsítványt létrehozva és a "Microsoft Root Authority" (CA) alá betagozódva módosított Microsoft update állományokat írnak alá, akkor a Microsoft azonnali hatállyal kitörölte az összes MD5-alapú CA tanúsítványt az operációs rendszereinek kulcstáraiból. Vajon lesz-e most ilyen akció, látva, hogy inkább pont ennek az ellenkezőjéért (a határidő 2016. december 31-re való kiterjesztéséért) megy a lobby ("The purpose of the ballot is to allow the issuance of SHA-1 certificates through 2016, with maximum Expiry Date of 31 December 2016.")?