

Re: [Full-disclosure] Internet Explorer Crash

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-04/msg00543.html>

- *From:* Valdis.Kletnieks@xxxxxx
 - *Date:* Wed, 18 Apr 2007 12:55:51 -0400
-

On Wed, 18 Apr 2007 12:31:57 EDT, Kradorex Xeron said:

There should be an implimentation on ALL browsers that a loop such large is unacceptable and refuse to even run it. There is no viable reason for a client-side to run a loop through so many itterations.

There's this thing called the Turing Halting Problem. :)

The problem is that it's **really** hard to **programatically** look at a loop like that, and say "That's going to loop 'too long' (for some fuzzy definition of 'too long')". Take that same code, and change the comparison to 'while (z.length < 3)'. Does that loop "too long"? How about '< 8'? (Keep in mind that to check this **from within**, it needs to have the knowledge that z is the loop control, which it has, and that z.length is approximately log₁₀(z), and that some value of log₁₀(z) is "too much". And once you've coded all that knowledge, the attacker just changes the test to this:

```
while (foo(z) == TRUE) (...
```

and foo(z) is defined as:

```
boolean foo(int z) {
static a = 0;
if (isprime(z)) a++;
if a > 1000000 return FALSE;
return TRUE;
}
```

Bonus points for defining isprime() as "Sieve of Eratosthenes" rather than some higher-performance primality check like Rabin-Miller or similar. Or maybe not – Sieve is probably simple enough that you can special-case it, better methods have more obscure internals. And we're **trying** to burn CPU – so maybe "Sieve of Eratosthene's less clever brother" is called for (iterate 1 to N, rather than 1 to sqrt(N)) :)

So – other than "it has already burned more than N seconds of CPU", what test do you propose to make? And what do you do if the site is some Javascript-driven interface to a corporate application that the user is

Re: [Full-disclosure] Internet Explorer Crash

expected to be in all day, and it's *legitimate* to burn lots more than N seconds during an 8-hour day?

(Hint – "trusted site" is probably not the greatest way to phrase that sort of check... ;)

Attachment: [pgpXeNiHcyaI5.pgp](#)

Description: PGP signature

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>