

Heads Up: SSL defeated in IE and Konqueror

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2002-10/3684.html>

From: Hale (hale@nospam.mail.com)

Date: 08/13/02

From: Hale <hale@nospam.mail.com>

Date: Tue, 13 Aug 2002 07:56:54 GMT

Actual Page: <http://www.theregister.co.uk/content/4/26620.html>

SSL defeated in IE and Konqueror

By Thomas C Greene in Washington

Posted: 12/08/2002 at 06:38 GMT

A colossal stuff-up in Microsoft's and KDE's implementation of SSL (Secure Sockets Layer) certificate handling makes it possible for anyone with a valid VeriSign SSL site certificate to forge any other VeriSign SSL site certificate, and abuse hapless Konqueror and Internet Explorer users with impunity.

In more detail, we have a certificate chain issue discovered by Mike Benham of thoughtcrime.org. A chain is formed when an intermediate certificate is trusted between server and client. Supposedly, the intermediate is accepted only if it's signed by the certificate authority as safe for the purpose. If it's merely signed by another certificate's key, it ought not to be trusted, or at least the user should be warned. Unfortunately, due to a preposterous security engineering oversight, IE and Konqueror don't bother to check this, so if a tricky site owner signs an intermediate cert with another valid cert, users will be none the wiser.

The browser, Benham says, "should verify that the CN [Common Name] field of the leaf certificate matches the domain it just connected to, that it's signed by the intermediate CA [Certificate Authority], and that the intermediate CA is signed by a known CA certificate. Finally, the Web browser should check that all intermediate certificates have valid CA basic constraints."

And it's here that IE fails. There's no checking of basic constraints. Thus an attacker can obtain a legitimate SSL cert for his domain and use it to sign a dummy cert for a second site. IE fails to check whether the dummy is in fact valid for the second site, but merely assumes that it is. More specifically, a cert which should not be used to sign others simply isn't checked. It's entirely possible to specify that a given cert is not valid to sign others; only IE will simply neglect to check if that's the case.

The wind-up is that any fool with an SSL cert can spoof certs for popular, trusted sites, and intercept communications widely imagined to be secure with a

man-in-the-middle attack. If this should happen to you, that reassuring little padlock icon is essentially worthless.

Benham has set up a demonstration using amazon.com as the spoofee. I gather he would prefer the test IP not be published, but he can be reached via email through his BugTraq posts. For the demonstration to work, the test IP and amazon have to be associated.

I've not tested this on IE because several researchers posting to Benham's BugTraq thread have confirmed the behavior. But I did test it on Mozilla 0.9.4, which Benham says isn't vulnerable, and Konqueror 3.0 (KDE 3.0.2 on SuSE 8.0), which he doesn't mention.

Konqueror turned out quite vulnerable, as I mentioned above. Mozilla was not vulnerable, but I'm not sure if that's because it handled the situation properly, or is, ironically, somehow too buggy to be exploited.

I made a simple HTML file with links to the amazon URL. After associating Benham's test-page IP with www.amazon.com in my hosts file I found that in Konqueror, following a link to <https://www.amazon.com> brought me immediately to the 'you've been hacked' page, indicating total failure. The behavior was the same when I typed the URL into the address bar.

With Mozilla the URL, <https://www.amazon.com> simply went nowhere. No cert warning, no 404, nothing. The browser simply remained on the page from which I started. The behavior was the same when I typed the URL into the address bar.

I honestly don't know if that qualifies as success or a felicitous failure; but either way Mozilla users can continue to use SSL in the mean time, while Microsoft and VeriSign are bickering and blaming each other for the problem. ®

-
- *Next message:* [Jon Smith III: "Re: Bummer! What to do now?"](#)
 - *Previous message:* [Saxeksknockers.edu: "Re: Snort reports strange port scans"](#)
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)