

## [VulnWatch] IE chain vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-01/0033.html>

---

**From:** Alex Loots ([a.loots@itsec-ss.nl](mailto:a.loots@itsec-ss.nl))

**Date:** 01/22/03

Date: Wed, 22 Jan 2003 09:54:35 +0100

From: Alex Loots <[a.loots@itsec-ss.nl](mailto:a.loots@itsec-ss.nl)>

To: "[vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)" <[vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)>

Hello list,

I have noticed some strange behaviour regarding the IE certificate chain vulnerability reported in MS02-050. The patch that fixes this vulnerability results in strange behavior of IE when a connection attempt is being made to a website which uses a malicious certificate.

I have set up a demo that uses a malicious certificate (A) that is generated on 19-08-2002 by means of a website certificate (B) published by a default IE trusted third party (C). Certificate B is valid from 17-08-2002 until 16-11-2002. When I connect to the malicious website with the current date set on my client system (22-01-2003 at the time of this writing) the patched IE gives a warning about the validity date of the certificate and does not give any warnings regarding the faulty certificate chain. In my opinion IE should tell exactly why the certificate is not correct including the faulty chain. Most end users don't even bother the warning about the date and continue browsing. This happens all the time with valid certificates so they have seen it before.

When I set the date of my client system to a date between 19-08-2002 and 16-11-2002 it is not possible to connect to the malicious website. The default IE "DNS or ..." error page is being displayed. The error displayed is not informative enough but IE at least keeps me from entering the malicious site.

So even with a patched version of IE it is still possible to almost transparently exploit the chain vulnerability because of incorrect (date)-warnings.

I have tested this on a W2KPro system with a patched IE 5.0.

-Alex