

Report about CVE-2014-1771

Name:

CVE-2014-1771

Base Score:

No Information

Vector:

No Information

Description:

SChannel in Microsoft Internet Explorer 6 through 11 does not ensure that a server's X.509 certificate is the same during renegotiation as it was before renegotiation, which allows man-in-the-middle attackers to obtain sensitive information or modify TLS session data via a "triple handshake attack," aka "TLS Server Certificate Renegotiation Vulnerability."

Nist:

NVD

Source:

Microsoft Corporation

Publish time: 06/11/2014

Website link: <https://nvd.nist.gov/vuln/detail/CVE-2014-1771>

Exploit DB search link: <https://www.exploit-db.com/search?cve=2014-1771>