CVE: CVE-2014-1771

Publish time: 06/11/2014

Source: Microsoft Corporation

Base Score:

Vector:

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."

Hyperlinks (4):

Link1: http://www.securityfocus.com/bid/67861

Link2: http://www.securitytracker.com/id/1030370

Link3: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-035

Link4: https://secure-resumption.com/

CWE Names (1):

CWE-310