



## ICASI Advisory

**November 11, 2009**

### **Transport Layer Security (TLS) Man-In-The-Middle (MITM) Vulnerability CVE-2009-3555**

The Industry Consortium for Advancement of Security on the Internet (ICASI) is releasing this alert to provide guidance on an issue that was disclosed to the general public on November 5, 2009. A protocol-level design flaw allows for an attacker to perform a man-in-the-middle (MITM) attack on sessions protected by Transport Layer Security (TLS) and Secure Sockets Layer (SSL). This vulnerability could allow an attacker who is able to successfully leverage a MITM attack to prepend data to an SSL/TLS-protected session. It does not allow the attacker to read, decrypt, or alter encrypted traffic between client and server.

**Note:** This is not a cryptographic vulnerability in TLS, but rather a vulnerability in the way that TLS handles previously authenticated sessions. This means that although an attacker cannot actually read any of the session data, it may be possible to insert arbitrary data on behalf of either the client or server in specific scenarios. Users are only affected when an attacker is able to successfully exploit this vulnerability in conjunction with a MITM attack, such as a local subnet attack or DNS spoofing. This makes consistent and successful exploitation of the vulnerability unlikely.

**As of November 11, 2009, ICASI is not aware of any public exploit attempts but note that exploit code for this vulnerability has been released to the public. We will continue to work with our partners to monitor for active exploitation.**

#### **Mitigation Options:**

Users can take a number of actions to both mitigate this vulnerability and detect whether it is being exploited. ICASI recommends that organizations test all of the following mitigations before implementation:



*Mitigation Option 1 (server side):* Web sites that allow access by anonymous clients and later poll the client for a certificate when a protected resource is accessed may be more vulnerable to an attack. Moving from an anonymous to a mutually-authenticated state requires a server-initiated renegotiation which exposes the vulnerability. Web sites can be architected to require mutual authentication up front, which reduces the necessity for TLS renegotiation, as the certificate can be transferred in the initial SSL negotiation.

*Mitigation Option 2:* Exploitation of this vulnerability can be prevented by disabling renegotiation in the TLS session. Renegotiation can take place when initiated by either the TLS client or the TLS server, as follows:

- A client may initiate TLS renegotiation at any time throughout the data transfer. This may be done in order to refresh TLS keys or to renegotiate cryptographic requirements. Client-initiated renegotiation has limited use and is relatively uncommon.
- or
- The server may initiate TLS renegotiation when it is configured to support multiple cryptographic requirements for individual resources, or to request the client certificate from the TLS client when using mutual authentication.

Server administrators can prevent an attack if they have sufficient control over their server applications to disable TLS renegotiation, and the ability to refuse client-initiated renegotiation attempts. It should be noted that renegotiation has valid use scenarios and disabling renegotiation may have application compatibility implications.

*Mitigation Option 3:* TLS is used in a variety of administrative and management roles, ranging from network equipment to back end servers. Often system/network administrators rely on TLS for security, forgoing the deployment of access lists to limit the IP addresses that have access to administrative functions. By deploying

appropriate access list to the administrative and management functions that use TLS, organizations can reduce the "attack surface" of an MITM attack.

**Detection Options:**

To date, it has been observed that server side logging does not help detect the abuse of this vulnerability. In addition, much of the network traffic appears non-malicious and normal to most network devices. That said, the following detection options are available to help detect a potential attack:

*Detection Option 1:* Many network Intrusion Prevention Systems have the ability to identify SSL key renegotiation. This can be used to detect the potential exploitation of this vulnerability and in some cases these exploit attempts can be blocked. Note that the impact of blocking this traffic should be tested as it may cause adverse effects on certain clients or applications. Consult your vendor to see if they can perform this function.

*Detection Option 2:* Some network security devices support SSL decryption if the private keys are loaded onto the device. If the entire session can be decrypted by the network device, it is possible to detect an attack by capturing and blocking the injection of arbitrary HTTP data. Consult with the appropriate vendor for more information on this option.

*Detection Option 3:* Host-based security vendors may be able to offer detection of this vulnerability by monitoring for client initiation renegotiations and disallowing them. Note that this option may not provide complete detection and may have adverse effects on certain applications.

Security vendors are aware of this issue and may develop signatures and detection to help administrators and users prevent its exploitation. ICASI recommends that users ensure security software and devices are kept up-to-date to help protect against this vulnerability and other threats.



**Vendor Actions:**

ICASI is continuing research into this vulnerability and is considering all potential attack vectors and ways to detect and mitigate them. The TLS IETF working group is working on a draft extension to the protocol that is intended to address this issue.

For more information, please check the IETF TLS mailing list:

<http://www.ietf.org/dyn/wg/charter/tls-charter.html>

Please note that a high level of interoperability testing will be required by multiple vendors when updating to address this vulnerability. ICASI is committed to working with all vendors, operators, and CSIRTs (including non-ICASI members) to coordinate this testing and ensure that any protocol-wide changes work broadly. If your organization wishes to participate in the interoperability work, please contact ICASI through your official representative (e-mail to [usirp\\_chair@icasi.org](mailto:usirp_chair@icasi.org)).

**Vendor Status:**

We recommend that all organizations contact their respective vendors for testing and patching timelines. A number of ICASI vendors have proactively released the following public statements and advisories from other vendors will be included as they become available:

Cisco: <http://www.cisco.com/warp/public/707/cisco-sa-20091109-tls.shtml>

Juniper Networks:

<https://www.juniper.net/alerts/viewalert.jsp?actionBtn=Search&txtAlertNumber=PSN-2009-11-573&viewMode=view>

The open source community has responded with a mitigation to OpenSSL that will disable SSL renegotiation. Again, we highly recommend that organizations test this mitigation before rolling it out to production environments. More information is available at: <http://www.openssl.org/>

Press requests regarding this or any ICASI issue should be directed to [press@icasi.org](mailto:press@icasi.org) while requests of a technical nature or requests to join the



discussions on this issue should be directed to: [usirp\\_chair@icasi.org](mailto:usirp_chair@icasi.org). For patching information, please consult your appropriate vendor.