CVE-2014-5075 MitM Vulnerability in the Smack XMPP Library for Java

Georg Lukas, rt-solutions.de, 2014-08-05

Smack is an Open Source XMPP (Jabber) client library for instant messaging and presence written in Java. Smack prior to version 4.0.2 is vulnerable to TLS Man-in-the-Middle attacks, as it fails to check if the server certificate matches the hostname of the connection.

Affected versions

- Smack 4.0.0 and 4.0.1 are vulnerable.
- Smack 2.x and 3.x are vulnerable if a custom `SSLContext` is supplied via `connectionConfiguration.setCustomSSLContext()`.

Details

Smack is using Java's `SSLSocket`, which checks the peer certificate using an `X509TrustManager`, but does not perform hostname verification. Therefore, it is possible to redirect the traffic between a Smack-using application and a legitimate XMPP server through the attacker's server, merely by providing a valid certificate for a domain under the attacker's control.

In Smack versions 2.2.0 to 3.4.1, a custom `ServerTrustManager` implementation was used, which was supplied with the connection's server name, and performed hostname verification. However, it failed to verify the basicConstraints and nameConstraints of the certificate chain (CVE-2014-0363) and has been removed in Smack 4.0.0.

Applications using Smack 2.2.0 to 3.4.1 with a custom `TrustManager` did not benefit from `ServerTrustManager` and are vulnerable as well, unless their own `TrustManager` implementation explicitly performs hostname verification.

Mitigation

Users of the Smack library are advised to upgrade to Smack 4.0.2, and then use `connectionConfiguration.setHostnameVerifier()` with a reasonable `HostnameVerifier` implementation. A proper hostname verifier **MUST** be configured to close the vulnerability.

For Smack 3.x users, a backported commit has been created. Here, a `HostnameVerifier` implementation needs to be supplied via `connectionConfiguration.setHostnameVerifier`
as well.

When using the official JRE, the internal class `sun.security.util.HostnameChecker` can be wrapped as described here.

If Apache's HttpClient library is available, its `StrictHostnameVerifier` can be used.

On Android, MemorizingTrustManager provides both certificate checking and hostname verification with interactive fallback, allowing the user to decide about the trustworthiness of a server.

Affected Applications

Smack is a library used by different applications. Therefore, the authors of the following Smack-based applications have been contacted to coordinate updated releases:

- ChatSecure (fixed in 13.2.0-beta1)
- GTalkSMS (contacted on 2014-07-28)
- MAXS (tracker issue, fixed in 0.0.1.18)
- yaxim and Bruno (fixed in 0.8.8)
- *undisclosed Android application* (contacted on 2014-07-21)

The following Smack-based applications were not affected:

- TransVerse (special interest client)
- Xabber (using a custom `TrustManager` performing hostname verification)

Timeline

- 2014-07-20 Discovery of Smack vulnerability, notification of Smack maintainer
- 2014-07-21 Notification of vulnerable apps' authors
- 2014-07-27 Release of Smack 4.0.2
- 2014-08-01 Release of MAXS 0.0.1.18
- 2014-08-04 Release of yaxim 0.8.8
- 2014-08-05 Release of ChatSecure 13.2.0 beta 1
- 2014-08-05 Publication of this advisory

Links

Online version of advisory PDF version