rt-solutions.de
experts you can trust.

CVE-2017-5589+ Multiple XMPP Clients User Impersonation Vulnerability

Dr. Georg Lukas, rt-solutions.de, 2017-02-09

Classification:

- CWE-304: Missing Critical Step in Authentication
- CWE-940: Improper Verification of Source of a Communication Channel
- CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N (score 7.1)

Affected Applications

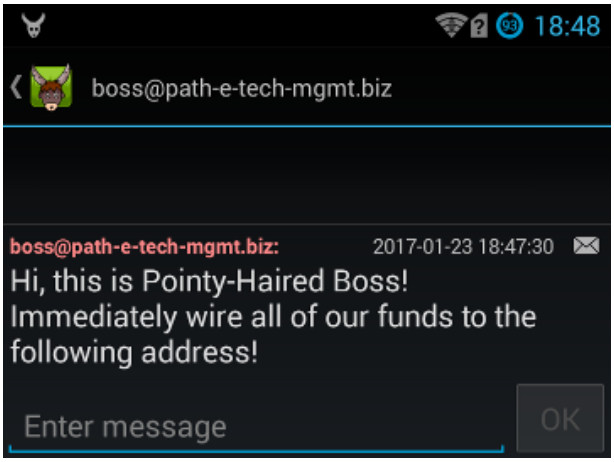
- CVE-2017-5589: yaxim and Bruno (0.8.6 - 0.8.8; Android)
- CVE-2017-5590: ChatSecure (3.2.0 - 4.0.0; iOS) and Zom (all versions up to 1.0.11; iOS)
- CVE-2017-5591: poezio (0.8 - 0.10)
- CVE-2017-5592: profanity (0.4.7 - 0.5.0)
- CVE-2017-5593: Psi+ (0.16.563.580 - 0.16.571.627)
- CVE-2017-5602: jappix (1.0.0 to 1.1.6)
- CVE-2017-5603: Jitsi (2.5.5061 - 2.9.5544)
- CVE-2017-5604: mcabber (1.0.0 - 1.0.4)
- CVE-2017-5605: Movim (0.8 - 0.10)
- CVE-2017-5606: Xabber (only if manually enabled: 1.0.30, 1.0.30 VIP, beta 1.0.3 - 1.0.74; Android)
- CVE-2017-5858: Converse.js (0.8.0 - 1.0.6, 2.0.0 - 2.0.4)

Affected Libraries

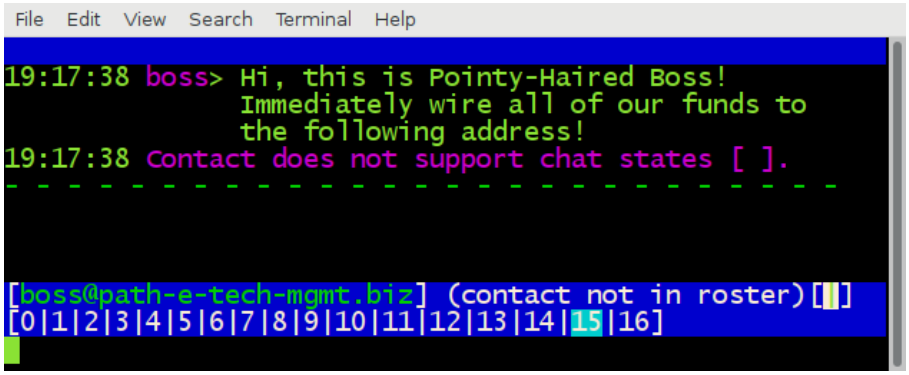
- CVE-2017-5591: SleekXMPP unknown up to 1.3.1
- CVE-2017-5591: Slixmpp all versions up to 1.2.3

Summary

An incorrect implementation of XEP-0280: Message Carbons in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks.



yaxim screenshot: impersonation of Pointy-Haired Boss by Mallory



poezio screenshot: impersonation of Pointy-Haired Boss by Mallory

Details

The XMPP protocol extension XEP-0280: Message Carbons allows a user to run multiple clients on their XMPP account by sending "carbon copies" of outgoing and incoming messages to the user's other devices (besides the one that directly sent or received the original message).

This feature must be supported by the user's server and must be explicitly enabled by the client. Carbon copies are always generated by the user's server and originate from the user's bare JID (their account address).

For example, the following is message "Hi!", sent by Alice (`alice@xmpp.example`) to Bob's client 1 (`bob@xmpp.example/client1`):

```
<message from="alice@xmpp.example" to="bob@xmpp.example/client1">
   <body>Hi!</body>
</message>
```

Bob is also logged in with carbons-enabled client 2, which receives the following carbon-copy of the message:

```
<message from="bob@xmpp.example" to="bob@xmpp.example/client2">
   <received xmlns='urn:xmpp:carbons:2'>
      <forwarded xmlns='urn:xmpp:forward:0'>
         <message from="alice@xmpp.example" to="bob@xmpp.example/client1">
            <body>Hi!</body>
         </message>
      </forwarded>
   </received>
</message>
```

Now, client 2 can extract the original message from the carbon copy and display it accordingly. The "Security Considerations" section of XEP-0280 explicitly states that:

> Any forwarded copies received by a Carbons-enabled client MUST be from that user's bare JID; any copies that do not meet this requirement MUST be ignored.

The Carbons implementation in the affected clients was lacking this test. It simply checked all incoming messages for presence of a Carbon element (`<received/>` or `<sent/>`), extracted and parsed it like a regular message.

Therefore, it was possible for Mallory to send the following specially crafted message to Bob:

```
<message from="mallory@evil.example" to="b@xmpp.example">
    <received xmlns='urn:xmpp:carbons:2'><forwarded xmlns='urn:xmpp:forwar
d:0'>
        <message from="alice@xmpp.example" to="bob@xmpp.example/client1">
            <body>Please come to Creepy Valley tonight, alone!</body>
        </message>
    </forwarded></received>
</message>
```

This would appear as an authentic message from Alice, including Alice' proper screen name, allowing Mallory to perform social engineering attacks on Bob.

Mitigation

While the attacker can send messages in the name of somebody else, they can not see your responses. Therefore, if you receive a phony message while using an affected client, reinsure with the message sender by either challenging them with a question that can not be guessed by the attacker, or by using out-of-band means.

Xabber: disable the experimental Carbons feature in the app settings.

yaxim: Disabling Message Carbons under "Settings" / "Edit account" / "Message Carbons (XEP-0280)" **will not solve the problem**, as the malicious messages still will be interpreted.

rt-solutions.de
experts you can trust.

Timeline

- 2017-01-20 Discovery of vulnerability
- 2017-01-23 - 26 Notification of developers
- 2017-01-25 Release of ChatSecure 4.0.1 (fix commit)
- 2017-01-26 Release of jappix 1.1.7 (fix commit)
- 2017-01-28 Release of Psi+ 0.16.571.630 (fix commit)
- 2017-01-29 Release of profanity 0.5.1 (fix commit)
- 2017-01-29 Release of mcabber 1.0.5 (fix commit)
- 2017-01-30 Release of poezio 0.11 with slixmpp 1.2.4 (slixmpp fix commit)
- 2017-01-31 Release of yaxim and Bruno 0.9.0 (fix commit)
- 2017-01-31 Release of Movim 0.11alpha1 (fix commit)
- 2017-01-31 Notification of Debian Security Team
- 2017-02-01 Release of profanity 0.4.7.patch1 and 0.5.0.patch1 (backports of the fix)
- 2017-02-01 Release of Converse.js 1.07 and 2.05 (fix commit)
- 2017-02-05 Release of Jitsi 2.10 (fix commit)
- 2017-02-08 Release of Zom 1.0.12 (fix commit)
- 2017-02-09 Publication of this advisory

Acknowledgements

- Daniel Gultsch for CVE-2015-8688: Gajim Roster Push Attack / Message Interception
- Sam Whited for CVE-2016-9928, same as above in mcabber
- Thijs Alkemade for being an awesome XMPP security researcher (and for proof-reading this)

Links

- Online version of advisory
- PDF version