Thunderbird/Enigmail SOS Fund Audit Fix Log

Identified Vulnerabilities

TBE-01-002 Enigmail: Weak Parsing causes Confidentiality Compromise (Critical)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1412631.
Patch:
https://sourceforge.net/p/enigmail/source/ci/927ddf0223f796f34040125f97e5b423f6573c9c/
Released as part of Enigmail 2.0.

Nikolai Krein (Cure53): *EnigmailFuncs.stripEmail() reliably errors out when emails contain an additional pair of <>. Manually verified.*

VERIFIED

TBE-01-005 Enigmail: Replay of encrypted Contents leads to Plaintext Leak (High)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1412632.
Patches:

- https://sourceforge.net/p/enigmail/source/ci/945a5f36c0817cad8bdf1c70112205a22502ee32
- https://sourceforge.net/p/enigmail/source/ci/8d3afec4f1c3c8faf4a6a93bf38cb508d17e6b7a

Released as part of Enigmail 2.0.

Nikolai Krein (Cure53): *Behaviour got changed completely. Embedded encrypted messages are not decrypted automatically but left as is if the encrypted part's sender does not match the current sender. Steps to reproduce fail.*

VERIFIED

TBE-01-011 Thunderbird: RSS Feed vulnerable against Email Injection (High)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411699.
Patch: https://bugzilla.mozilla.org/attachment.cgi?id=8927143.
Released as part of Thunderbird 59.0.

Nikolai Krein (Cure53): *Not authorized to view the patch! However, manually testing shows behaviour is different. Newlines are not interpreted and the injected email structure is not expanded.*

VERIFIED

TBE-01-012 Thunderbird: RSS Local Path Leak via @-moz-document (Medium)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411708
Patches:
https://hg.mozilla.org/mozilla-central/rev/37e0bd919af0
https://hg.mozilla.org/mozilla-central/rev/b556432c990b
Fixed in Thunderbird 59

Nikolai Krein (Cure53): *Cannot reproduce original bug on TB 58.0b1*, but patch is missing.
Mario Heiderich (Cure53): *Patch is now present, fix is verified*

VERIFIED

TBE-01-013 Thunderbird: RSS Local Path Leak via cid: Parsing Bug (Medium)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411713
No patch so far.

Nikolai Krein (Cure53): *Cannot reproduce original bug on TB 58.0b1, unable to import the feed containing the PoC, feed fails to validate. Patch is missing.*

VERIFIED

TBE-01-014 Thunderbird: JavaScript Execution via RSS in mailbox:// Origin (High)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411716.
Patches:
https://bugzilla.mozilla.org/attachment.cgi?id=8926442
https://bugzilla.mozilla.org/attachment.cgi?id=8927088
Fixed in Thunderbird 58.0.

Nikolai Krein (Cure53): *Not authorized to view the patch! However, JS is not executed, href in resulting base-tag is emptied:*
<base href=""> (fixed)
Vs
<base href="data:text/html,%3ch1%3…(vuln)

VERIFIED

TBE-01-015 Thunderbird: Decrypted PGP Blocks exposed via RSS Feeds (Critical)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411718.
The way TBE-01-011 and TBE-01-014 were fixed, there was nothing more to fix for the issue here.

Nikolai Krein (Cure53): *015 depends on previous issues to be valid, however they are fixed.*

VERIFIED

TBE-01-017 Thunderbird: Multiple Hangs via malformed Headers (Medium)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411720

VERIFIED

Mario Heiderich (Cure53): *Added regex as well as the test-cases look good, verified!*

TBE-01-021 Enigmail: Flawed parsing allows faked Signature Display (Critical)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1412633.
Patches:
- https://sourceforge.net/p/enigmail/source/ci/698cc370b5094937b63aacb07e407f42f38542ca/
- https://sourceforge.net/p/enigmail/source/ci/284e9408145126e55db8e2c4a37111c9dd5ef0e2/

Released as part of Enigmail 2.0.

Nikolai Krein (Cure53): *Behaviour upon receiving attached files that are signed is changed and the enigmail message for a good signature is not displayed any more.*

VERIFIED

Miscellaneous Issues

TBE-01-001 Enigmail: Insecure Random Secret Generation (Low)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1412636.
Patch:
https://sourceforge.net/p/enigmail/source/ci/f221d4d92f5d06c7d33c3a57d815b5a7d147a220
Release as part of Enigmail 2.0.

Nikolai Krein (Cure53): *As advised, Math.random() is replaced with crypto.getRandomValues().*

VERIFIED

TBE-01-003 Enigmail: Regular Expressions Exploitable for Denial of Service (Low)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1412637.
Patch:
https://sourceforge.net/p/enigmail/source/ci/eeb340604663e2a15459831af1acd2b97787b547/
Release as part of Enigmail 2.0.

Nikolai Krein (Cure53): *All mentioned regexes are now length restricted.*

VERIFIED

TBE-01-004 Enigmail: Autocrypt Automatic Key Import (Info)

(no concrete action to take)

Nikolai Krein (Cure53): *Autocrypt is in still developement, future will tell if the recommendations were taken into consideration.*

NO ACTION TO TAKE

TBE-01-007 Thunderbird: JavaScript Execution via Reload Page Dialog (Low)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411748

Nikolai Krein (Cure53): *No change, PoC works and XSS is triggered.*

UNFIXED

TBE-01-008 Enigmail: Default Keyserver configured without SSL (Info)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1412638.
Patch:
https://sourceforge.net/p/enigmail/source/ci/a14c50b1da9ecd39ceded7e34f7137778102a625
Part of Enigmail 2.0

Nikolai Krein (Cure53): *Uses hkps:// now.*

VERIFIED

TBE-01-009 Thunderbird: Filename Spoofing for external Attachments (Info)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411732.
Fixed as part of TBE-01-014.

Nikolai Krein (Cure53): *The GUI still displays the filename that is outlined in the content-type header. Considering unfixed.*

UNFIXED (Update: Fixed on 2018-04-27)

This is the response of the Thunderbird developers:
For the record, it is completely legitimate to have a display name. This is no different from a web page text link where the text could be some spoofy wording to evilsite.com url. Since only http links are accepted now, a click will open the url in a default browser whose infrastructure for handling malicious sites takes over.

The enhancement needed is to enable the user to at least see the url link, like in Firefox.

TBE-01-010 Thunderbird: DoS via invalid X-Mozilla-Draft-Info header (Low)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411734.
Patch: https://bugzilla.mozilla.org/attachment.cgi?id=8922686
Fixed in Thunderbird 57.0, foreseen for Thunderbird 52.5.0

Nikolai Krein (Cure53): *Code is fine now null deref is prevented with the correct branch. Manually verified, crash does not happen.*

VERIFIED

TBE-01-006 Thunderbird: Denial of Service via Link to .eml Attachment (Low)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411735.

VERIFIED

Mario Heiderich (Cure53): *The diff was reviewed, the cause of the crash was removed.*

TBE-01-016 Thunderbird: DoS via proprietary X-Mozilla-Cloud-Part Header (Low)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411737.
Patch: https://bugzilla.mozilla.org/attachment.cgi?id=8923076
Fixed in Thunderbird 58.0, foreseen for Thunderbird 52.5.0

Nikolai Krein (Cure53): *Code is fine now, and manually verified, crash does not happen.*

VERIFIED

TBE-01-018 Thunderbird: Integer and Heap-Overflow in MIME-Body-Parsing (High)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411741.
Fixed as part of bug https://bugzilla.mozilla.org/show_bug.cgi?id=1392052.
Patch: https://bugzilla.mozilla.org/attachment.cgi?id=8900023
Fixed in Thunderbird 57.0

Nikolai Krein (Cure53): *Code received a complete overhaul.*

VERIFIED

TBE-01-019 Thunderbird: Integer Overflow in Attachment Code (High)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411744.
Patch: https://bugzilla.mozilla.org/attachment.cgi?id=8922364
Fixed in Thunderbird 58.0

Nikolai Krein (Cure53): *Not authorized to view the patch! Checked via GIT: bodyLen is now limited to < UINT32_MAX, so wrapping to 0 should not happen.*

VERIFIED

TBE-01-020 Thunderbird: Null Pointer Exception via SVG and Mailbox URI (Info)

Filed as https://bugzilla.mozilla.org/show_bug.cgi?id=1411745
Patch: https://bugzilla.mozilla.org/attachment.cgi?id=8933938
Fixed in Thunderbird 59

VERIFIED