



CVE-2020-15953

Published on: 07/27/2020 12:00:00 AM UTC

Last Modified on: 01/20/2023 09:03:00 PM UTC

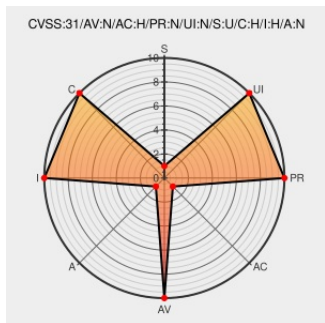
CVE-2020-15953

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

LibEtPan through 1.9.4, as used in MailCore 2 through 0.6.3 and other products, has a STARTTLS buffering issue that affects IMAP, SMTP, and POP3. When a server sends a "begin TLS" response, the client reads additional data (e.g., from a meddler-in-the-middle attacker) and evaluates it in a TLS context, aka "response injection."

CVE-2020-15953 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.4 - HIGH**

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|------------------|------------------------|---------------------|---------------------|
| NETWORK | HIGH | NONE | NONE |
| Scope | Confidentiality Impact | Integrity Impact | Availability Impact |
| UNCHANGED | HIGH | HIGH | NONE |

CVSS2 Score: **5.8 - MEDIUM**

| Access Vector | Access Complexity | Authentication |
|------------------------|-------------------|---------------------|
| NETWORK | MEDIUM | NONE |
| Confidentiality Impact | Integrity Impact | Availability Impact |
| PARTIAL | PARTIAL | NONE |

CVE References

| Description | Tags | Link |
|--|---|---|
| [security-announce] openSUSE-SU-2020:1505-1: moderate: Security update f | lists.opensuse.org text/html | SUSE openSUSE-SU-2020:1505 |
| Buffering issues with STARTTLS in IMAP - Issue #386 | Exploit | MISC: github.com/dinhvh/libetpan/issues/386 |

Buffering issues with STARTTLS handling - Issue #600
dinhvh/libetpan · GitHub

[Exploit](#)
[Patch](#)
[Third Party Advisory](#)
[github.com](#)
[text/html](#)

[CVE-2020-1454](#) [github.com](#) [libetpan](#) [#600](#)

libetpan: Improper STARTTLS handling (GLSA 202007-55) —
Gentoo security

[Third Party Advisory](#)
[security.gentoo.org](#)
[text/html](#)

 [GENTOO GLSA-202007-55](#)


[security-announce] openSUSE-SU-2020:1454-1: moderate:
Security update f

[lists.opensuse.org](#)
[text/html](#)

 [SUSE openSUSE-SU-2020:1454](#)

[SECURITY] [DLA 2329-1] libetpan security update

[lists.debian.org](#)
[text/html](#)

 [MLIST \[debian-lts-announce\] 20200816](#)
[\[SECURITY\] \[DLA 2329-1\] libetpan security update](#)

[SECURITY] Fedora 32 Update: libetpan-1.9.4-4.fc32 -
package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org](#)
[text/html](#)

 [FEDORA FEDORA-2020-13ae5f7221](#)

[SECURITY] Fedora 31 Update: libetpan-1.9.3-3.fc31 -
package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org](#)
[text/html](#)

 [FEDORA FEDORA-2020-44e52ef729](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[501598](#) Alpine Linux Security Update for libetpan

Exploit/POC from Github

LibEtPan through 1.9.4, as used in MailCore 2 through 0.6.3 and other products, has a STARTTLS buffering issue that a...

Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|----------------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 31 | All | All | All |
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Application | Libetpan Project | Libetpan | All | All | All | All |
| Application | Libmailcore | Mailcore2 | All | All | All | All |

[cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:](#)

[cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:](#)

[cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:](#)

[cpe:2.3:a:libetpan_project:libetpan:*:*:*:*:*:](#)

cpe:2.3:a:libmailcore:mailcore2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)