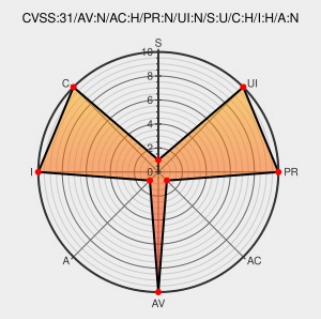
CVE-2020-15953

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 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 in IMAP · Issue #000 dinhvh/libetpan · GitHub	Exploit Patch Third Party Advisory github.com text/html	MISC github.com/dinhvh/libetpan/issues/000
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

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→