Security Advisory 2019-019

Critical Exim TLS Vulnerability

September 09, 2019 — v1.0

TLP:WHITE

History:

- *09/19/2019 — v1.0 – Initial publication*

Summary

Exim Mail Transfer Agent (MTA) servers are exposed to a security vulnerability, which can grant attackers the ability to run malicious code with root privileges. This vulnerability has been assigned the number CVE-2019-15846 [1, 9]. The vulnerability is particularly critical, as over 50% of MTAs in the world use Exim [4].

Technical Details

The vulnerability allows local or unauthenticated remote attackers to execute programs with root privileges on affected servers that accept TLS connections. The vulnerability is exploitable by sending a Server Name Indication (SNI) ending in a backslash-null sequence during the initial TLS handshake [2]. The vulnerability only depends if the server accepts TLS connections. It does not depend on the TLS library, so both, GnuTLS and OpenSSL are affected. An exploit POC already exists [5].

Products Affected

- All Exim servers running version 4.92.1 and before are vulnerable.

Recommendations

Download and build a fixed version 4.92.2 [6, 7, 8, 9].

If the above versions cannot be directly installed, contact your package maintainer for a version containing the backported fix [9].

Possible Workarounds

Server owners can mitigate this vulnerability by disabling TLS support for the Exim server. However, this may not be an option, as this exposes email traffic in cleartext, and makes it vulnerable to sniffing attacks and interception [6].

References

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15846

[2] https://github.com/Exim/exim/blob/exim-4.92.2%2Bfixes/doc/doc-txt/cve-2019-15846/cve.txt

[3] https://www.zdnet.com/article/millions-of-exim-servers-vulnerable-to-root-granting-exploit/8

[4] http://www.securityspace.com/s_survey/data/man.201905/mxsurvey.html

[5] https://github.com/Exim/exim/blob/exim-4.92.2%2Bfixes/doc/doc-txt/cve-2019-15846/qualys.mbx

[6] https://github.com/Exim/exim/blob/exim-4.92.2%2Bfixes/doc/doc-txt/cve-2019-15846/cve.txt

[7] https://ftp.exim.org/pub/exim/exim4/

[8] https://github.com/Exim/exim.git

[9] http://exim.org/static/doc/security/CVE-2019-15846.txt