

# Dovecot Assessment

---

To determine the scope of the Dovecot assessment, Cigital employed an abbreviated threat modeling process. This process was used to identify key targets in the application that could yield interesting results. For the purposes of this assessment, Cigital identified only the external facing input mechanisms as targets of interest.

A technique known as fuzzing was performed on the externally exposed mail protocols (LMTP, POP3 and IMAP). This involved sending data to be interpreted by the protocols in an attempt to cause unexpected application behavior. Test data sent from one tool included standard alphanumeric characters as well as the three core control characters (null byte, line feed and carriage return). Using this character set, strings of data were constructed randomly from the size of 1 character to 4098 characters. Another tool sent protocol specific requests with abnormally large datasets and/or unexpected parameters. Dovecot did not exhibit any insecure or unwanted behavior when under load from the fuzzing tools. Behavior was observed using the Wireshark network monitoring utility, and by performing actions as an authorized user; these actions were unaffected by testing. Also employed in testing were hooks. These hooks were applied to common functions used for inter-process communication (IPC), and acted as proxies to record and relay the data sent from the calling function to the hooked function. No.

Finally, a code review was conducted to determine if the application source contained weaknesses that can lead to exploitable vulnerabilities. The review focused on manual analysis of the memory management routines in the code, as well as common problems reported by the static analysis tools listed on the SAMATE page for Dovecot. In addition, Cigital included results from the clang static analysis tool (part of the LLVM project). Common problems were identified by comparing the output of each static analysis tool to the output of the others to determine if any of the tools identified the same weaknesses. While common weaknesses were identified, no weakness was determined to be exploitable by an external attacker on a Dovecot system configured using default security constraints.