Remote Code Execution via Shell Injection in qmail-remote TLS Error Handler #42

Merged **sagredo-dev** merged 2 commits into `main` from `qmail-remote-injection-fix` last week

Conversation 0 Commits 2 Checks 0 Files changed 2

sagredo-dev commented last week — Owner

Thanks to Diep Pham, who spotted this vulnerability.

When an outbound TLS handshake fails, `qmail-remote` automatically records the remote hostname in a blocklist file by executing a shell command constructed from the unsanitized DNS MX exchange name. An attacker who controls DNS records for a domain can embed shell metacharacters in the MX hostname, achieving arbitrary command execution on the mail server as the `qmailr` user. The vulnerability requires the `control/notlshosts_auto` feature to be enabled (a documented production feature for handling broken TLS hosts) and for the victim server to send or relay email to the attacker-controlled domain.

sagredo-dev added 2 commits 2 weeks ago

`[security] Remote Code Execution via Shell Injection in qmail-remote …` ··· `749f607`

`qmail dir is calculated in create_notlshost_file function` `b71b5ae`

sagredo-dev merged commit **`122b803`** into `main` last week

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

1 participant