History · Edit

RUSTSEC-2021-0069

SMTP command injection in body

Reported	May 22, 2021
Issued	May 22, 2021 (last modified: October 19, 2021)
Package	lettre (crates.io)
Type	Vulnerability
Categories	format-injection
Keywords	#email #smtp
Aliases	GHSA-qc36-q22q-cjw3 CVE-2021-38189
Details	https://github.com/lettre/lettre/pull/627/commits/93458d01fed0ec81c0e7b4e98e6f35961356fae2

Patched	`>=0.10.0-rc.3`
	`<0.10.0-alpha.1, >=0.9.6`

Unaffected	`<0.7.0`

Affected Functions	Version
`lettre::smtp::SmtpTransport::send`	`<0.10.0-alpha.1`
`lettre::transport::smtp::SmtpTransport::send`	`>=0.10.0-alpha.1, <0.10.0-rc.3`
`lettre::transport::smtp::SmtpTransport::send_raw`	`>=0.10.0-alpha.1, <0.10.0-rc.3`

Description

Affected versions of lettre allowed SMTP command injection through an attacker's controlled message body. The module for escaping lines starting with a period wouldn't catch a period that was placed after a double CRLF sequence, allowing the attacker to end the current message and write arbitrary SMTP commands after it.

The flaw is fixed by correctly handling consecutive CRLF sequences.