# CVE Detail – CVE-2020-3812

qmail-verify as used in netqmail 1.06 is prone to an information disclosure vulnerability. A local attacker can test for the existence of files and directories anywhere in the filesystem because qmail-verify runs as root and tests for the existence of files in the attacker's home directory, without dropping its privileges first.

## Threat-Mapped Scoring

Score: 2.3

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.13899

## CVSS Scoring

CVSS v3.1 Score: 5.5

Severity: MEDIUM

## Mapped CWE(s)

* CWE-269: Improper Privilege Management

## CAPEC(s)

* CAPEC-122: Privilege Abuse
* CAPEC-233: Privilege Escalation
* CAPEC-58: Restful Privilege Elevation

## ATT&CK Techniques

* T1548: Abuse Elevation Control Mechanism

## Used By (Actors/Tools)

* Raspberry Robin (malware)

## Affected Products

* cpe:2.3:a:netqmail:netqmail:1.06:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:8.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:9.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:10.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:20.04:\*:\*:\*:lts:\*:\*:\*