

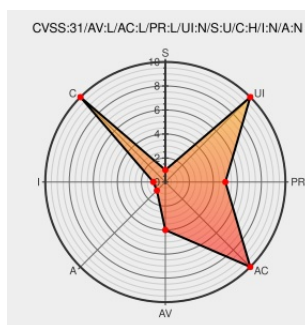


CVE-2020-3812

Published on: 05/26/2020 12:00:00 AM UTC

Last Modified on: 04/28/2022 07:30:00 PM UTC

CVE-2020-3812

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

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.

CVE-2020-3812 has been assigned by security@debian.org to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Debian** - **netqmail** version **1.06**

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-4692-1 netqmail	Third Party Advisory	MISC www.debian.org/security/2020/dsa-4692

www.debian.org[Deprecated Link](#)[text/html](#)

USN-4556-1: netqmail vulnerabilities | Ubuntu security notices | Ubuntu

usn.ubuntu.com[text/html](#) [UBUNTU USN-4556-1](#)

oss-security - Remote Code Execution in qmail (CVE-2005-1513)

[Exploit](#)[Mailing List](#)[Patch](#)[Third Party Advisory](#)www.openwall.com[text/html](#) [CONFIRM N/A](#)

#961060 - qmail-verify: CVE-2020-3811 CVE-2020-3812 - Debian Bug report logs

[Issue Tracking](#)[Third Party Advisory](#)bugs.debian.org[text/html](#) [MISC bugs.debian.org/961060](https://bugs.debian.org/961060)

[SECURITY] [DLA 2234-1] netqmail security update

lists.debian.org[text/html](#) [MLIST \[debian-lts-announce\] 20200604 \[SECURITY\] \[DLA 2234-1\] netqmail security update](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netqmail	Netqmail	1.06	All	All	All
Application	Netqmail	Netqmail	1.06	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:20.04:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:

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:debian:debian_linux:9.0:*****:
cpe:2.3:a:netqmail:netqmail:1.06:*****:
cpe:2.3:a:netqmail:netqmail:1.06:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous ID		Next ID→