



CVE-2020-3811

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

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

CVE-2020-3811

[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 a mail-address verification bypass vulnerability.

CVE-2020-3811 has been assigned by [@ security@debian.org](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [@ Debian](#) - **netqmail** version **1.06**

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

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

Exploit-DB
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

[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	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: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→

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)