



CVE-2005-1513

Published on: 05/11/2005 12:00:00 AM UTC

Last Modified on: 06/08/2023 05:15:00 PM UTC

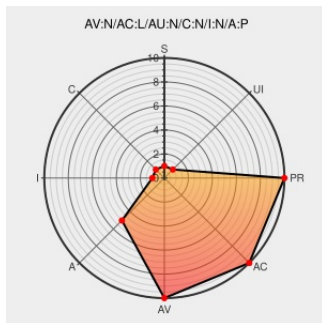
CVE-2005-1513

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Qmail](#) from [Dan Bernstein](#) contain the following vulnerability:

Integer overflow in the stralloc_readplus function in qmail, when running on 64 bit platforms with a large amount of virtual memory, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a large SMTP request.

CVE-2005-1513 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

RenderDoc 1.26 Local Privilege Escalation / Remote Code Execution ≈ Packet Storm

[packetstormsecurity.com](#)
[text/html](#)

MISC [packetstormsecurity.com/files/172804/RenderDoc-1.26-Local-Privilege-Escalation-Remote-Code-Execution.html](#)

Qmail Local Privilege Escalation / Remote Code Execution ≈ Packet Storm

[packetstormsecurity.com](#)
[text/html](#)

MISC [packetstormsecurity.com/files/158203/Qmail-Local-Privilege-Escalation-Remote-Code-Execution.html](#)

Debian -- Security Information -- DSA-4692-1 netqmail

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

DEBIAN DSA-4692

Qualys Security Advisory - Qmail Remote Code Execution ≈ Packet Storm

[packetstormsecurity.com](#)
[text/html](#)

MISC [packetstormsecurity.com/files/157805/Qualys-Security-Advisory-Qmail-Remote-Code-Execution.html](#)

Neohapsis Archives - Full Disclosure List - #0101 - [Full-disclosure] 64 bit qmail fun

[Exploit](#)
[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

FULLDISC 20050506 64 bit qmail fun

netqmail: Multiple vulnerabilities (GLSA 202007-01) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-202007-01
oss-security - Re: Remote Code Execution in qmail (CVE-2005-1513)	www.openwall.com text/html	 MLIST [oss-security] 20200520 Re: Remote Code Execution in qmail (CVE-2005-1513)
64 bit qmail fun	Exploit www.guninski.com text/html	 MISC www.guninski.com/where_do_you_want_billg_to_go_today_4.html
Full Disclosure: Remote Code Execution in qmail (CVE-2005-1513)	seclists.org text/html	 FULLDISC 20200522 Remote Code Execution in qmail (CVE-2005-1513)
oss-security - Re: Remote Code Execution in qmail (CVE-2005-1513)	www.openwall.com text/html	 MLIST [oss-security] 20200616 Re: Remote Code Execution in qmail (CVE-2005-1513)
qmail Integer Errors Let Remote Users Deny Service - SecurityTracker	Exploit securitytracker.com text/html	 SECTrack 1013911
USN-4556-1: netqmail vulnerabilities Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	 UBUNTU USN-4556-1
oss-security - Re: Remote Code Execution in qmail (CVE-2005-1513)	www.openwall.com text/html	 MLIST [oss-security] 20200520 Re: Remote Code Execution in qmail (CVE-2005-1513)
Full Disclosure: LPE and RCE in RenderDoc: CVE-2023-33865, CVE-2023-33864, CVE-2023-33863	seclists.org text/html	 FULLDISC 20230607 LPE and RCE in RenderDoc: CVE-2023-33865, CVE-2023-33864, CVE-2023-33863
oss-security - Remote Code Execution in qmail (CVE-2005-1513)	www.openwall.com text/html	 MLIST [oss-security] 20200519 Remote Code Execution in qmail (CVE-2005-1513)
[SECURITY] [DLA 2234-1] netqmail security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20200604 [SECURITY] [DLA 2234-1] netqmail security update
oss-security - LPE and RCE in RenderDoc: CVE-2023-33865, CVE-2023-33864, CVE-2023-33863	www.openwall.com text/html	 MLIST [oss-security] 20230606 LPE and RCE in RenderDoc: CVE-2023-33865, CVE-2023-33864, CVE-2023-33863
Full Disclosure: Re: Remote Code Execution in qmail (CVE-2005-1513)	seclists.org text/html	 FULLDISC 20200623 Re: Remote Code Execution in qmail (CVE-2005-1513)

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
Application	Dan Bernstein	Qmail	All	All	All	All
Application	Dan Bernstein	Qmail	All	All	All	All
<pre>cpe:2.3:a:dan_bernstein:qmail:*****:</pre>						
<pre>cpe:2.3:a:dan_bernstein:qmail:*****:</pre>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netsec	15 years later, bugs were never fixed: Remote Code Execution in qmail (CVE-2005-1513)	2020-05-20 01:41:16
 /r/YourselfYou	Qualys Security Advisory 15 years later: Remote Code Execution in qmail (CVE-2005-1513)	2020-05-19 19:52:41

[← 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](#)