



CVE-2004-2163

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2163

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

Certain versions of [Openbsd](#) from [Openbsd](#) contain the following vulnerability:

login_radius on OpenBSD 3.2, 3.5, and possibly other versions does not verify the shared secret in a response packet from a RADIUS server, which allows remote attackers to bypass authentication by spoofing server replies.

CVE-2004-2163 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Secunia - Advisories - OpenBSD Radius Authentication "login_radius" Security Bypass

[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[X](#) [SECUNIA 12617](#)

Neohapsis Archives - VulnWatch - #0058 - [VulnWatch] OpenBSD radius authentication vulnerability

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

[VULNWATCH 20040921 OpenBSD radius authentication vulnerability](#)

OpenBSD Radius Authentication Bypass Vulnerability

[Patch](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 11227](#)

OpenBSD 3.5 errata

[Patch](#)
[www.openbsd.org](#)
[text/html](#)

[CONFIRM](#)
[www.openbsd.org/errata35.html#radius](#)

404 Not Found

Patch

Vendor Advisory

www.reseau.nl

text/plain

Inactive Link

Not Archived

MISC

www.reseau.nl/advisories/0400-openbsd-radius.txt

No Description Provided

www.osvdb.org

Inactive Link

Not Archived

OSVDB 10203

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

text/html

XF openbsd-radius-auth-bypass(17456)

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	Openbsd	Openbsd	3.2	All	All	All
Operating System	Openbsd	Openbsd	3.4	All	All	All
Operating System	Openbsd	Openbsd	3.5	All	All	All
Operating System	Openbsd	Openbsd	3.2	All	All	All
Operating System	Openbsd	Openbsd	3.4	All	All	All
Operating System	Openbsd	Openbsd	3.5	All	All	All
cpe:2.3:o:openbsd:openbsd:3.2:*:*:*:*:*:						
cpe:2.3:o:openbsd:openbsd:3.4:*:*:*:*:*:						
cpe:2.3:o:openbsd:openbsd:3.5:*:*:*:*:*:						
cpe:2.3:o:openbsd:openbsd:3.2:*:*:*:*:*:						
cpe:2.3:o:openbsd:openbsd:3.4:*:*:*:*:*:						
cpe:2.3:o:openbsd:openbsd:3.5:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [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](#)