



# CVE-2018-1160

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2018-1160
<b>State</b>	PUBLIC
<b>Assigner</b>	vulnreport@tenable.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-20 21:29:00 UTC
<b>Updated</b>	2023-09-29 11:15:00 UTC
<b>Description</b>	Netatalk before 3.1.12 is vulnerable to an out of bounds write in dsi_opensess.c. This is due to lack of bounds checking on

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netatalk	Netatalk	All	All	All	All
Application	Netatalk Project	Netatalk	All	All	All	All
Application	Netatalk Project	Netatalk	All	All	All	All
Application	Synology	Diskstation Manager	All	All	All	All
Application	Synology	Diskstation Manager	All	All	All	All
Application	Synology	Router Manager	All	All	All	All
Application	Synology	Router Manager	All	All	All	All
Application	Synology	Skynas	-	All	All	All
Application	Synology	Skynas	-	All	All	All
Hardware	Synology	Vs960hd	-	All	All	All
Hardware	Synology	Vs960hd	-	All	All	All
Operating System	Synology	Vs960hd Firmware	-	All	All	All
Operating System	Synology	Vs960hd Firmware	-	All	All	All

## References

Reference	Source	Link	Tags
QNAP Netatalk Authentication Bypass ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	Exploit, Third Party A
Netatalk 3.1.12 - Authentication Bypass (PoC) - Multiple dos Exploit	EXPLOIT-DB	<a href="https://www.exploit-db.com">www.exploit-db.com</a>	Exploit, Third Party A
<a href="https://attachments.samba.org/attachment.cgi">attachments.samba.org/attachment.cgi</a>	MISC	<a href="https://attachments.samba.org">attachments.samba.org</a>	Third Party Advisory
Netatalk 3.1.12 - Authentication Bypass - Multiple remote Exploit	EXPLOIT-DB	<a href="https://www.exploit-db.com">www.exploit-db.com</a>	Exploit, Third Party A
Debian -- Security Information -- DSA-4356-1 netatalk	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Third Party Advisory
Netatalk Release Notes	CONFIRM	<a href="https://netatalk.sourceforge.net">netatalk.sourceforge.net</a>	Release Notes
QNAP Netatalk < 3.1.12 - Authentication Bypass - Multiple remote Exploit	EXPLOIT-DB	<a href="https://www.exploit-db.com">www.exploit-db.com</a>	Exploit, Third Party A
<a href="https://poc/netatalk/cve_2018_1160">poc/netatalk/cve_2018_1160</a> at master · tenable/poc · GitHub	MISC	<a href="https://github.com">github.com</a>	Release Notes, Third
Synology Inc.	CONFIRM	<a href="https://www.synology.com">www.synology.com</a>	Third Party Advisory
Netatalk CVE-2018-1160 Arbitrary Code Execution Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory,
[R2] Netatalk Out-of-bounds Write - Research Advisory   Tenable®	MISC	<a href="https://www.tenable.com">www.tenable.com</a>	Exploit, Release Note
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[501093](#) Alpine Linux Security Update for netatalk

[505086](#) Alpine Linux Security Update for netatalk

[690248](#) Free Berkeley Software Distribution (FreeBSD) Security Update for netatalk3 (9c9023ff-9057-11e9-b764-00505632d232)

© [CVE.report](https://cve.report) 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)