CVE-2018-1160

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-1160
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-20 21:29:00 UTC
Updated	2023-09-29 11:15:00 UTC
Description	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	packetstormsecurity.com	Exploit, Third Party Ac
Netatalk 3.1.12 - Authentication Bypass (PoC) - Multiple dos Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit, Third Party Ac
attachments.samba.org/attachment.cgi	MISC	attachments.samba.org	Third Party Advisory
Netatalk 3.1.12 - Authentication Bypass - Multiple remote Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit, Third Party Ac
Debian -- Security Information -- DSA-4356-1 netatalk	DEBIAN	www.debian.org	Third Party Advisory
Netatalk Release Notes	CONFIRM	netatalk.sourceforge.net	Release Notes
QNAP Netatalk < 3.1.12 - Authentication Bypass - Multiple remote Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit, Third Party Ac
poc/netatalk/cve_2018_1160 at master · tenable/poc · GitHub	MISC	github.com	Release Notes, Third
Synology Inc.	CONFIRM	www.synology.com	Third Party Advisory
Netatalk CVE-2018-1160 Arbitrary Code Execution Vulnerability	BID	www.securityfocus.com	Third Party Advisory,
[R2] Netatalk Out-of-bounds Write - Research Advisory | Tenable®	MISC	www.tenable.com	Exploit, Release Note
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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)