



CVE-2017-9078

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-9078
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-19 14:29:00 UTC
Updated	2022-07-11 17:11:00 UTC
Description	The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double fre

Risk And Classification

Problem Types: CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Dropbear Ssh Project	Dropbear Ssh	All	All	All	All
Application	Dropbear Ssh Project	Dropbear Ssh	All	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-3859-1 dropbear	DEBIAN	www.debian.org	Third I
September 2019 Dropbear SSH Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
Dropbear 2017.75	CONFIRM	lists.ucc.gu.uwa.edu.au	Mailing
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#) 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](#)