



CVE-2017-18766

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

Summary

CVE	CVE-2017-18766
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-22 16:15:00 UTC
Updated	2020-04-24 19:50:00 UTC
Description	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects DST6501 before 1.1.0.6 a

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Dst6501	-	All	All	All
Hardware	Netgear	Dst6501	-	All	All	All
Operating System	Netgear	Dst6501 Firmware	All	All	All	All
Operating System	Netgear	Dst6501 Firmware	All	All	All	All
Hardware	Netgear	Wnr2000	v2	All	All	All
Hardware	Netgear	Wnr2000	v2	All	All	All
Operating System	Netgear	Wnr2000 Firmware	All	All	All	All
Operating System	Netgear	Wnr2000 Firmware	All	All	All	All

References

Reference	Source	Link
Security Advisory for Arbitrary File Read on DST6501 and WNR2000v2, PSV-2017-0425 Answer NETGEAR Support	CONFIRM	kb.netgear.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)