



CVE-2020-35225

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

Summary

CVE	CVE-2020-35225
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-10 18:15:00 UTC
Updated	2021-03-15 19:45:00 UTC
Description	The NSDP protocol implementation on NETGEAR JGS516PE/GS116Ev2 v2.6.0.43 devices was not properly validating the

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Gs116e	v2	All	All	All
Hardware	Netgear	Gs116e	v2	All	All	All
Operating System	Netgear	Gs116e Firmware	2.6.0.43	All	All	All
Operating System	Netgear	Gs116e Firmware	2.6.0.43	All	All	All
Hardware	Netgear	Jgs516pe	-	All	All	All
Hardware	Netgear	Jgs516pe	-	All	All	All
Operating System	Netgear	Jgs516pe Firmware	2.6.0.43	All	All	All
Operating System	Netgear	Jgs516pe Firmware	2.6.0.43	All	All	All

References

Reference	Source
Technical Advisory – Multiple Vulnerabilities in Netgear ProSAFE Plus JGS516PE / GS116Ev2 Switches – NCC Group Research	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)