



CVE-2017-18790

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

Summary

CVE	CVE-2017-18790
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-21 19:15:00 UTC
Updated	2020-04-27 16:23:00 UTC
Description	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R6700 before 1.0.1.26, R7000 b

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	R6700	-	All	All	All
Hardware	Netgear	R6700	-	All	All	All
Operating System	Netgear	R6700 Firmware	All	All	All	All
Operating System	Netgear	R6700 Firmware	All	All	All	All
Hardware	Netgear	R7000	-	All	All	All
Hardware	Netgear	R7000	-	All	All	All
Operating System	Netgear	R7000 Firmware	All	All	All	All
Operating System	Netgear	R7000 Firmware	All	All	All	All
Hardware	Netgear	R7100lg	-	All	All	All
Hardware	Netgear	R7100lg	-	All	All	All
Operating System	Netgear	R7100lg Firmware	All	All	All	All
Operating System	Netgear	R7100lg Firmware	All	All	All	All
Hardware	Netgear	R7900	-	All	All	All
Hardware	Netgear	R7900	-	All	All	All
Operating System	Netgear	R7900 Firmware	All	All	All	All
Operating System	Netgear	R7900 Firmware	All	All	All	All
Hardware	Netgear	R8000	-	All	All	All

Hardware	Netgear	R8000	-	All	All	All
Operating System	Netgear	R8000 Firmware	All	All	All	All
Operating System	Netgear	R8000 Firmware	All	All	All	All
Hardware	Netgear	R8500	-	All	All	All
Hardware	Netgear	R8500	-	All	All	All
Operating System	Netgear	R8500 Firmware	All	All	All	All
Operating System	Netgear	R8500 Firmware	All	All	All	All

References						
Reference						Source
Security Advisory for Sensitive Information Disclosure Vulnerability on Some Routers, PSV-2017-0317 Answer NETGEAR Support						CONFIRMED
CVE Program record						CVE ID
NVD vulnerability detail						NVD

No vendor comments have been submitted for this CVE.

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