CVE-2017-6366

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-6366
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-15 14:59:00 UTC
Updated	2017-03-29 14:03:00 UTC
Description	Cross-site request forgery (CSRF) vulnerability in NETGEAR DGN2200 routers with firmware 10.0.0.20 through 10.0.0.50 a

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Dgn2200v1	-	All	All	All
Hardware	Netgear	Dgn2200v1	-	All	All	All
Hardware	Netgear	Dgn2200v2	-	All	All	All
Hardware	Netgear	Dgn2200v2	-	All	All	All
Hardware	Netgear	Dgn2200v3	-	All	All	All
Hardware	Netgear	Dgn2200v3	-	All	All	All
Hardware	Netgear	Dgn2200v4	-	All	All	All
Hardware	Netgear	Dgn2200v4	-	All	All	All
Operating System	Netgear	Dgn2200 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Netgear DGN2200v1/v2/v3/v4 - Cross-Site Request Forgery - Hardware webapps Exploit	EXPLOIT-DB	www.exploit-db.com	Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report