CVE-2016-11014

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-11014
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-16 11:15:00 UTC
Updated	2020-11-10 19:40:00 UTC
Description	NETGEAR JNR1010 devices before 1.0.0.32 have Incorrect Access Control because the ok value of the auth cookie is a sp

Risk And Classification

Problem Types: CWE-613

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Jnr1010	-	All	All	All
Hardware	Netgear	Jnr1010	-	All	All	All
Operating System	Netgear	Jnr1010 Firmware	All	All	All	All
Operating System	Netgear	Jnr1010 Firmware	All	All	All	All

References

Reference	Source	Lir
CVE-2016-11014 - Authentication Bypass in Netgear Router	MISC	cyb
Authentication Bypass in Netgear Router JNR1010 Version 1.0.0.24 · Issue #14 · cybersecurityworks/Disclosed · GitHub	MISC	gith
Netgear 1.0.0.24 Bypass / Improper Session Management ≈ Packet Storm	MISC	pac
full-disclosure - [FD] Broken Authentication & Improper Session Management in Netgear Router JNR1010 Version 1.0.0.24	MISC	list
Free Facebook Scripts Extensions	MISC	kha
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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