CVE-2019-5016

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

Summary

CVE	CVE-2019-5016
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-17 21:15:00 UTC
Updated	2022-06-13 18:40:00 UTC
Description	An exploitable arbitrary memory read vulnerability exists in the KCodes NetUSB.ko kernel module which enables the Ready

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kcodes	Netusb.ko	1.0.2.66	All	All	All
Application	Kcodes	Netusb.ko	1.0.2.69	All	All	All
Application	Kcodes	Netusb.ko	1.0.2.66	All	All	All
Application	Kcodes	Netusb.ko	1.0.2.69	All	All	All
Hardware	Netgear	R7900	-	All	All	All
Hardware	Netgear	R7900	-	All	All	All
Operating System	Netgear	R7900 Firmware	1.0.3.810.037	All	All	All
Operating System	Netgear	R7900 Firmware	1.0.3.810.037	All	All	All
Hardware	Netgear	R8000	-	All	All	All
Hardware	Netgear	R8000	-	All	All	All
Operating System	Netgear	R8000 Firmware	1.0.4.28_10.1.54	All	All	All
Operating System	Netgear	R8000 Firmware	1.0.4.28_10.1.54	All	All	All

References

Reference	Source	Link	Tags
TALOS-2019-0775 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	Third Party
Malformed Request	BID	www.securityfocus.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.