CVE-2015-3036

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

Summary

CVE	CVE-2015-3036
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-21 01:59:00 UTC
Updated	2016-12-08 03:08:00 UTC
Description	Stack-based buffer overflow in the run_init_sbus function in the KCodes NetUSB module for the Linux kernel, as used in ce

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kcodes	Netusb	-	All	All	All
Application	Kcodes	Netusb	-	All	All	All

References

Reference	Sou
Linux/MIPS Kernel 2.6.36 - 'NetUSB' Remote Code Execution - Multiple remote Exploit	EXP
KCodes NetUSB CVE-2015-3036 Buffer Overflow Vulnerability	BID
Full Disclosure: SEC Consult SA-20150519-0 :: Critical buffer overflow vulnerability in KCodes NetUSB (VU#177092, CVE-2015-3036)	FUL
NetUSB - Kernel Stack Buffer Overflow - Hardware dos Exploit	EXP
SEC Consult: KCodes NetUSB: How a Small Taiwanese Software Company Can Impact the Security of Millions of Devices Worldwide	MIS
KCodes NetUSB Buffer Overflow ≈ Packet Storm	MIS
Full Disclosure: Exploit NetUSB CVE-2015-3036	FUL
NETGEAR Router KCodes NetUSB Driver Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SEC
Vulnerability Lab - SEC Consult	MIS
Vulnerability Note VU#177092 - KCodes NetUSB kernel driver is vulnerable to buffer overflow	CEF
NetUSB Stack Buffer Overflow ≈ Packet Storm	MIS
CVE Program record	CVE

No vendor comments have been submitted for this CVE.

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