CVE-2015-5536

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

Summary

CVE	CVE-2015-5536
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-13 14:59:08 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Belkin N300 Dual-Band Wi-Fi Range Extender with firmware before 1.04.10 allows remote authenticated users to execute a

Risk And Classification

Primary CVSS: v2.0 9 from nvd@nist.gov

AV:N/AC:L/Au:S/C:C/I:C/A:C

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Belkin	N300 Dual-band Wi-fi Range Extender	All	All	All	All

Operating System	Belkin	N300 Dual-band Wi-fi Range Extender Firmware	1.0.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Belkin N300 Dual-Band Wi-Fi Range Extender Multiple Remote Code Execution Vulnerabilities
Zero Day Initiative
Official Belkin Support Site | N300 Dual-Band Wi-Fi Range Extender F9K1111 - Firmware
Zero Day Initiative
Zero Day Initiative
Zero Day Initiative
Belkin N300 Dual-Band Wi-Fi Range Extender Flaw Lets Remote Authenticated Users Execute Arbitrary Commands on the Target System - S
Zero Day Initiative
Zero Day Initiative
Zero Day Initiative
Zero Day Initiative
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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