



VDB-355402 · CVE-2026-5611 · GCVE-100-355402

BELKIN F9K1015 1.00.10 FORMCROSSBANDSWITCH WEBPAGE STACK- BASED OVERFLOW



Summary

A vulnerability described as [critical](#) has been identified in [Belkin F9K1015 1.00.10](#). This vulnerability affects the function `formCrossBandSwitch` of the file `/goform/formCrossBandSwitch`. Executing a manipulation of the argument `webpage` can lead to stack-based overflow. This vulnerability is tracked as [CVE-2026-5611](#). The attack can be launched remotely. Moreover, an exploit is present. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability classified as critical was found in [Belkin F9K1015 1.00.10](#). This vulnerability affects the function `formCrossBandSwitch` of the file `/goform/formCrossBandSwitch`. The manipulation of the argument `webpage` with an unknown input leads to a stack-based overflow vulnerability. The CWE definition for the vulnerability is [CWE-121](#). A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or, rarely, a parameter to a function). As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is available at [github.com](#). This vulnerability was named [CVE-2026-5611](#). The exploitation appears to be easy. The attack can be initiated remotely. Technical details and also a public exploit are known.

It is possible to download the exploit at [github.com](#). It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Product

Vendor

- [Belkin](#)

Name

- [F9K1015](#)

Version

- [1.00.10](#)

License

- [commercial](#)

CPE 2.3

- 

CPE 2.2

- 

CVSSv4

VulDB Vector: 

VulDB Reliability: 

CVSSv3

VulDB Meta Base Score: 8.8

VulDB Meta Temp Score: 8.0

VulDB Base Score: 8.8

VulDB Temp Score: 8.0

VulDB Vector: 

VulDB Reliability: 

CVSSv2

VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Stack-based overflow

CWE: [CWE-121](#) / [CWE-119](#)

CAPEC: 🔒

ATT&CK: 🔒

Physical: No

Local: No

Remote: Yes

Availability: 🔒

Access: Public

Status: Proof-of-Concept

Download: 🔒

Price Prediction: 🔍

Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍

Active Actors: 🔍

Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known

Status: 🔍

0-Day Time: 🔒

Timeline

04/05/2026		Advisory disclosed
04/05/2026	+0 days	VulDB entry created
04/05/2026	+0 days	VulDB entry last update

Sources

Advisory: [github.com](#)

Status: Not defined

CVE: [CVE-2026-5611](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5611](#)

GCVE (VulDB): [GCVE-100-355402](#)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

Entry

Created: 04/05/2026 05:35 PM

Changes: 04/05/2026 05:35 PM (57)

Complete: 🔍

Submitter: [LtzHust](#)

Cache ID: 52:E8C:179

Submit

Accepted

- [Submit #785538](#): Belkin F9K1015 1.00.10 Stack-based Buffer Overflow (by LtzHust)

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)