



VDB-355416 · CVE-2026-5628 · GCVE-100-355416

BELKIN F9K1015 1.00.10 SETTING FORMSETSYSTEMSETTINGS WEBPAGE STACK-BASED OVERFLOW



CVSS Meta Temp Score

8.0

Current Exploit Price (≈)

\$0-\$5k

CTI Interest Score

2.82

Summary

A vulnerability described as **critical** has been identified in **Belkin F9K1015 1.00.10**. The affected element is the function `formSetSystemSettings` of the file `/goform/formSetSystemSettings` of the component `Setting Handler`. The manipulation of the argument `webpage` results in stack-based overflow. This vulnerability is identified as **CVE-2026-5628**. The attack can be executed remotely. Additionally, an exploit exists. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability was found in **Belkin F9K1015 1.00.10**. It has been classified as **critical**. Affected is the function `formSetSystemSettings` of the file `/goform/formSetSystemSettings` of the component `Setting Handler`. The manipulation of the argument `webpage` with an unknown input leads to a stack-based overflow vulnerability. CWE is classifying the issue as **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). This is going to have an impact on confidentiality, integrity, and availability.

The advisory is shared for download at github.com. This vulnerability is traded as **CVE-2026-5628**. The exploitability is told to be easy. It is possible to launch the attack remotely. Technical details and a public exploit are known.

The exploit is shared for download 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-2026-5628](#) (🗝️)

GCVE (CVE): [GCVE-0-2026-5628](#)

GCVE (VulDB): [GCVE-100-355416](#)

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

Entry

Created: 04/05/2026 09:09 PM

Changes: 04/05/2026 09:09 PM (58)

Complete: 🔍

Submitter: [LtzHuster](#)

Cache ID: 52:01B:179

Submit

Accepted

- [Submit #785555](#): Belkin F9K1015 1.00.10 Stack-based Buffer Overflow (by LtzHuster)

Discussion

No comments yet. Languages: en.

Please [log in](#) to comment.

