

Instantly share code, notes, and snippets.

[k6dpvrmm8z-glitch](#) / [gist:7db9fb648a18ffcd8600bea436486884](#)

Created 19 hours ago

[Code](#) [Revisions](#) 1

CVE-2026-30363: Potential Stack Overflow in main (flipperzero-firmware)

[gistfile1.txt](#)

```
1 # CVE-2026-30363: Potential Stack Overflow in main (flipperzero-firmware)
2
3 ## Summary
4 A potential stack overflow vulnerability exists in the main function due to insufficient s
5
6 ## Affected Versions
7 - flipperzero-firmware (commit ad2a800 and possibly earlier versions)
8
9 ## Description
10 The main function is created with a fixed stack size of 1024 bytes:
11
12     _stack_size = 0x400; /* required amount of stack */
13
14 However, static stack usage analysis indicates that the worst-case call chain may require
15
16 This mismatch between allocated and required stack size may lead to a potential stack over
17
18 ## Impact
19 This issue may lead to:
20 - System crash
21 - Undefined behavior
22
23 ## Proof of Concept
24 1. Enable stack usage analysis:
25     - Add `-fstack-usage` to compiler flags
26 2. Build the project
27 3. Inspect generated `.su` files
28 4. Observe that main call chain exceeds allocated stack size
29
30 ## References
31 - https://github.com/flipperdevices/flipperzero-firmware/issues/4332
```