k6dpvrmm8z-glitch / **gist:7db9fb648a18ffcd8600bea436486884**

Created 17 hours ago

Code Revisions 1

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

gistfile1.txt

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

## Summary
A potential stack overflow vulnerability exists in the main function due to insufficient s

## Affected Versions
- flipperzero-firmware (commit ad2a800 and possibly earlier versions)

## Description
The main function is created with a fixed stack size of 1024 bytes:

    _stack_size = 0x400; /* required amount of stack */

However, static stack usage analysis indicates that the worst-case call chain may require

This mismatch between allocated and required stack size may lead to a potential stack over

## Impact
This issue may lead to:
- System crash
- Undefined behavior

## Proof of Concept
1. Enable stack usage analysis:
   - Add `-fstack-usage` to compiler flags
2. Build the project
3. Inspect generated `.su` files
4. Observe that main call chain exceeds allocated stack size

## References
- https://github.com/flipperdevices/flipperzero-firmware/issues/4332
```