# Integer Overflow in FileUplink (Critical)

Low **bitWarrior** published **GHSA-qmvv-rxh4-ccqh** last week

**Package**

**Svc/FileUplink/FileUplink.cpp** (F Prime)

| Affected versions | Patched versions |
| --- | --- |
| v4.1.1 | v4.2 |

**Description**

## Impact

- File: Svc/FileUplink/FileUplink.cpp, line 135
- Type: CWE-190 (Integer Overflow) → CWE-787 (Out-of-Bounds Write)
- Issue: The bounds check byteOffset + dataSize > fileSize uses U32 addition that wraps around on overflow. An attacker-crafted DataPacket with byteOffset=0xFFFFFF9C and dataSize=100 overflows to 0,
  bypassing the check entirely. The subsequent file write proceeds at the original ~4GB offset.
- Additional finding: Svc/FileUplink/File.cpp:20-31 performs no sanitization on the destination file path (CWE-22, Path Traversal). Combined, these allow writing arbitrary data to any file at any offset.
- Impact: Arbitrary file write → Remote Code Execution on embedded targets.
- Note: This is a logic bug. ASAN does not detect it because all memory accesses are within valid buffers
  — the corruption occurs in file I/O.

## Patches

This issue was resolved in Git Commit bb585fe

## Workarounds

No.

### Severity

Low 0.0 / 10

**CVSS v3 base metrics**

| | |
|---|---|
| Attack vector | Network |
| Attack complexity | Low |
| Privileges required | None |
| User interaction | None |
| Scope | Unchanged |
| Confidentiality | None |
| Integrity | None |
| Availability | None |

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

### CVE ID

CVE-2026-41144

### Weaknesses

- CWE-190
- CWE-787