Vulnerability Report Document

Document Information

Date: 2025-01-15T10:00:00Z

Tools:
- Dependency-Track (4.12.0)

Component name : Test Container ()

BOM Format: CycloneDX
Specification Version: 1.5
Version: 1
Serial Number: urn:uuid:b2896d3a-f7a1-47dc-a611-0f4f67643536

Vulnerabilities

1. ID: **CVE-2014-2893**
   Description: The GetHTMLRunDir function in the scan-build utility in Clang 3.5 and earlier allows local users to obtain sensitive information or overwrite arbitrary files via a symlink attack on temporary directories with predictable names.
   - **Severity:** low (CVSSv2 — Source: NVD)

2. ID: **CVE-2019-14871**
   Description: The REENT_CHECK macro (see newlib/libc/include/sys/reent.h) as used by REENT_CHECK_TM, REENT_CHECK_MISC, REENT_CHECK_MP and other newlib macros in versions prior to 3.3.0, does not check for memory allocation problems when the DEBUG flag is unset (as is the case in production firmware builds).
   - **Severity:** medium (CVSSv2 — Source: NVD)
   - **Severity:** medium (CVSSv3 — Source: NVD)

3. ID: **CVE-2019-14872**
   Description: The _dtoa_r function of the newlib libc library, prior to version 3.3.0, performs multiple memory allocations without checking their return value. This could result in NULL pointer dereference.
   - **Severity:** medium (CVSSv2 — Source: NVD)
   - **Severity:** medium (CVSSv3 — Source: NVD)

4. ID: **CVE-2019-14873**
   Description: In the __multadd function of the newlib libc library, prior to versions 3.3.0 (see newlib/libc/stdlib/mprec.c), Balloc is used to allocate a big integer, however no check is performed to verify if the allocation succeeded or not. This will trigger a null pointer dereference bug in case of a memory allocation failure.
   - **Severity:** medium (CVSSv2 — Source: NVD)
   - **Severity:** medium (CVSSv3 — Source: NVD)

5. ID: **CVE-2019-14874**
   Description: In the __i2b function of the newlib libc library, all versions prior to 3.3.0 (see newlib/libc/stdlib/mprec.c), Balloc is used to allocate a big integer, however no check is performed to verify if the allocation succeeded or not. The access of _ x[0] will trigger a null pointer dereference bug in case of a memory allocation failure.
   - **Severity:** medium (CVSSv2 — Source: NVD)
   - **Severity:** medium (CVSSv3 — Source: NVD)

6. ID: **CVE-2019-14875**

Description: In the __multiply function of the newlib libc library, all versions prior to 3.3.0 (see newlib/libc/stdlib/mprec.c), Balloc is used to allocate a big integer, however no check is performed to verify if the allocation succeeded or not. The access of _x[0] will trigger a null pointer dereference bug in case of a memory allocation failure.

- **Severity:** medium (CVSSv2 — Source: NVD)
- **Severity:** medium (CVSSv3 — Source: NVD)

7. ID: **CVE-2019-14876**
   Description: In the __lshift function of the newlib libc library, all versions prior to 3.3.0 (see newlib/libc/stdlib/mprec.c), Balloc is used to allocate a big integer, however no check is performed to verify if the allocation succeeded or not. The access to b1 will trigger a null pointer dereference bug in case of a memory allocation failure.

   - **Severity:** medium (CVSSv2 — Source: NVD)
   - **Severity:** medium (CVSSv3 — Source: NVD)

8. ID: **CVE-2019-14877**
   Description: In the __mdiff function of the newlib libc library, all versions prior to 3.3.0 (see newlib/libc/stdlib/mprec.c), Balloc is used to allocate big integers, however no check is performed to verify if the allocation succeeded or not. The access to _wds and _sign will trigger a null pointer dereference bug in case of a memory allocation failure.

   - **Severity:** medium (CVSSv2 — Source: NVD)
   - **Severity:** medium (CVSSv3 — Source: NVD)

9. ID: **CVE-2019-14878**
   Description: In the __d2b function of the newlib libc library, all versions prior to 3.3.0 (see newlib/libc/stdlib/mprec.c), Balloc is used to allocate a big integer, however no check is performed to verify if the allocation succeeded or not. Accessing _x will trigger a null pointer dereference bug in case of a memory allocation failure.

   - **Severity:** medium (CVSSv2 — Source: NVD)
   - **Severity:** medium (CVSSv3 — Source: NVD)

10. ID: **CVE-2021-3420**
    Description: A flaw was found in newlib in versions prior to 4.0.0. Improper overflow validation in the memory allocation functions mEMALIGn, pvALLOc, nano_memalign, nano_valloc, nano_pvalloc could case an integer overflow, leading to an allocation of a small buffer and then to a heap-based buffer overflow.

    - **Severity:** high (CVSSv2 — Source: NVD)
    - **Severity:** critical (CVSSv3 — Source: NVD)