Talos Vulnerability Report

TALOS-2020-1194

Micrium uC-HTTP HTTP Server null pointer dereference denial-of-service vulnerability

JANUARY 26, 2021

CVE NUMBER

CVE-2020-13583

Summary

A denial-of-service vulnerability exists in the HTTP Server functionality of Micrium uC-HTTP 3.01.00. A specially crafted HTTP request can lead to denial of service. An attacker can send an HTTP request to trigger this vulnerability.

Tested Versions

Micrium uC-HTTP 3.01.00

Product URLs

https://www.micrium.com/rtos/tcpip/

CVSSv3 Score

8.6 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

CWE

CWE-476 - NULL Pointer Dereference

Details

The uC-HTTP server implementation is designed to be used on embedded systems that are running the µC/OS II or µC/OS III RTOS kernels. This HTTP server supports many features including persistent connections, form processing, chunked transfer encoding, HTTP header fields processing, HTTP query string processing and dynamic content.

The HTTP server implementation provides compile time configuration options to enable HTTP Forms. By default the server will have this compiler option enabled but the developer is expected to set the `FormCfgPtr` structure at compile time. If this structure isn't set, then a denial of service exists due to a NULL pointer dereference when trying to access memory that is allocated based on the existence of the `FormCfgPtr` structure.

This code snippet shows the behavior of the code if the compiler flags `HTTPs_CFG_FORM_EN` and `HTTPs_CFG_FORM_MULTIPART_EN` are set, and the `FormCfgPtr` is NULL, memory will not be allocated for the `FormBoundaryPtr` variable. This snippet is from the function `HTTPsMem_ConnGet`

```
#if ((HTTPs_CFG_FORM_EN           == DEF_ENABLED) && \
     (HTTPs_CFG_FORM_MULTIPART_EN == DEF_ENABLED))
    if (p_cfg->FormCfgPtr != DEF_NULL) {

        if (p_cfg->FormCfgPtr->MultipartEn == DEF_ENABLED) {
                                                                /* ------------- ACQUIRE FORM BOUNDARY BLK ------------ */
            p_conn->FormBoundaryPtr = (CPU_CHAR *)Mem_DynPoolBlkGet(&p_instance->PoolFormBoundary,
                                                                    &err_lib);
```

Later, when processing Content Type multipart, the code attempts to place a null character at the end of a string pointed to by the pointer `FormBoundaryPtr`. The code does not check for a NULL pointer for either of the values `FormCfgPtr` or `FormBoundaryPtr` , which results in a NULL pointer dereference when `FormBoundaryPtr` is used. This is a code snippet from the function `HTTPsReq_HdrParse`

```
  /* Copy boundary val to Conn struct.                    */
                    Str_Copy_N(p_conn->FormBoundaryPtr,
                               p_val,
                               len);
                                        /* Make sure to create a string.                        */
                    p_conn->FormBoundaryPtr[len] = ASCII_CHAR_NULL;
```

Crash Information

```
Program received signal SIGSEGV, Segmentation fault.
HTTPsReq_HdrParse (p_err=0xffffcd48, p_conn=0x565a7708 <Mem_Heap+1352>, p_instance=0x565a71dc <Mem_Heap+28>) at http-s_req.c:1664
1664                                    p_conn->FormBoundaryPtr[len] = ASCII_CHAR_NULL;
(gdb) bt
#0  HTTPsReq_HdrParse (p_err=0xffffcd48, p_conn=0x565a7708 <Mem_Heap+1352>, p_instance=0x565a71dc <Mem_Heap+28>) at http-s_req.c:1664
#1  HTTPsReq_Handle (p_instance=0x565a71dc <Mem_Heap+28>, p_conn=0x565a7708 <Mem_Heap+1352>) at http-s_req.c:325
#2  0x56560ca2 in HTTPsConn_Process (p_instance=0x565a71dc <Mem_Heap+28>) at http-s_conn.c:159
#3  0x56564c21 in HTTPsTask_InstanceTaskHandler (p_instance=0x565a71dc <Mem_Heap+28>) at http-s_task.c:814
#4  HTTPsTask_InstanceTask (p_data=0x565a71dc <Mem_Heap+28>) at http-s_task.c:653
#5  0x565653a5 in HTTPsTask_InstanceTaskCreate (p_instance=0x565a71dc <Mem_Heap+28>, p_err=0xffffce78) at http-s_task.c:331
#6  0x5655ee96 in HTTPs_InstanceStart (p_instance=0x565a71dc <Mem_Heap+28>, p_err=0xffffce78) at http-s.c:811
#7  0x5659f0ce in AppNoFS_Init () at ../Examples/NoFS/app/app_no_fs.c:122
#8  0x56557326 in main (argc=1, argv=0xffffcf44) at ../Examples/NoFS/app/app_no_fs.c:133
```

Timeline

2020-11-02 - Vendor Disclosure
2021-01-22 - Vendor Patched
2021-01-26- Public Release

CREDIT

Discovered by Kelly Leuschner of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1193

NEXT REPORT TALOS-2020-1190
