Talos Vulnerability Report

TALOS-2020-1193

Micrium uC-HTTP HTTP Server unchecked return value denial-of-service vulnerability

JANUARY 26, 2021

CVE NUMBER

CVE-2020-13582

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-690 - Unchecked Return Value to 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 includes support for parsing multipart forms. When looking for the `=` token within the boundary parameter, the code does not check the return value of `Str_Char_N` which returns a NULL pointer when the character is not found in the provided string. The pointer returned from `Str_Char_N` is incremented and then passed to the function `HTTP_StrGraphSrcFirst` which attempts to dereference this pointer whose value is `0x01` and results in invalid memory access. Below is the vulnerable piece of code found in the function `HTTPsReq_HdrParse` :

```
/* Boundary located after '='.                          */
p_val = Str_Char_N(p_val, len, ASCII_CHAR_EQUALS_SIGN);
p_val++;              /* Remove space before boundary val.                    */
p_val = HTTP_StrGraphSrchFirst(p_val,
                               len);
```

Crash Information

```
Program received signal SIGSEGV, Segmentation fault.
HTTP_StrGraphSrchFirst (p_str=0x1 <error: Cannot access memory at address 0x1>, str_len=65530) at ../../Common/http.c:157
157         while ((ASCII_IS_GRAPH(*p_char) == DEF_NO) &&
(gdb) bt
#0  HTTP_StrGraphSrchFirst (p_str=0x1 <error: Cannot access memory at address 0x1>, str_len=65530) at ../../Common/http.c:157
#1  0x5655d07d in HTTPsReq_HdrParse (p_err=0xffffcd48, p_conn=0x565a7708 <Mem_Heap+1352>, p_instance=0x565a71dc <Mem_Heap+28>) at http-
s_req.c:1655
#2  HTTPsReq_Handle (p_instance=0x565a71dc <Mem_Heap+28>, p_conn=0x565a7708 <Mem_Heap+1352>) at http-s_req.c:325
#3  0x56560ca2 in HTTPsConn_Process (p_instance=0x565a71dc <Mem_Heap+28>) at http-s_conn.c:159
#4  0x56564c21 in HTTPsTask_InstanceTaskHandler (p_instance=0x565a71dc <Mem_Heap+28>) at http-s_task.c:814
#5  HTTPsTask_InstanceTask (p_data=0x565a71dc <Mem_Heap+28>) at http-s_task.c:653
#6  0x565653a5 in HTTPsTask_InstanceTaskCreate (p_instance=0x565a71dc <Mem_Heap+28>, p_err=0xffffce78) at http-s_task.c:331
#7  0x5655ee96 in HTTPs_InstanceStart (p_instance=0x565a71dc <Mem_Heap+28>, p_err=0xffffce78) at http-s.c:811
#8  0x5659f0ce in AppNoFS_Init () at ../Examples/NoFS/app/app_no_fs.c:122
#9  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-2020-1174

NEXT REPORT
TALOS-2020-1194