Talos Vulnerability Report

TALOS-2020-1188

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

JANUARY 5, 2021

CVE NUMBER

CVE-2020-13577

Summary

A denial-of-service vulnerability exists in the WS-Security 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 wsse plugin for supporting the WS-Security specification. While procesing a RequestSecurityToken request, a denial of service condition can be triggered when processing XML namespaces. If the namespace was previuosly included and has no value, a null pointer dereference can occur.

```
13866   if ((soap->mode & SOAP_XML_CANONICAL))
13867   {
13868     /* push namespace */
13869     if (!strncmp(name, "xmlns", 5) && ((name[5] == ':') || name[5] == '\0'))
13870     {
13871       (void)soap_push_ns(soap, name + 5 + (name[5] == ':'), value, 0, 0); <------ value is null and never checked before being saved.
13872       if (name[5] == '\0')
13873         soap_utilize_ns(soap, SOAP_STR_EOS, 0);
13874       else if (soap->c14ninclude && ((*soap->c14ninclude == '*' || soap_tagsearch(soap->c14ninclude, name + 6))))
13875         soap_utilize_ns(soap, name, 0);
13876     }
```

Crash Information

```
Starting program: /gsoap-2.8/gsoap/samples/wst/wstdemo ns 8080
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Server started at port 8080
Accepting connection from IP 127.0.0.1

Program received signal SIGSEGV, Segmentation fault.
__strcmp_ssse3 () at ../sysdeps/x86_64/multiarch/../strcmp.S:174
174     ../sysdeps/x86_64/multiarch/../strcmp.S: No such file or directory.
(gdb) bt
#0  __strcmp_ssse3 () at ../sysdeps/x86_64/multiarch/../strcmp.S:174
#1  0x00005555555b25f8 in soap_push_ns (soap=soap@entry=0x7ffff7fba010, id=0x55555583ef16 "SOAP-ENV", ns=ns@entry=0x0,
utilized=utilized@entry=0, isearly=isearly@entry=0)
    at ../../stdsoap2.c:12677
#2  0x00005555555b614d in soap_attribute (soap=soap@entry=0x7ffff7fba010, name=<optimized out>, name@entry=0x55555583ef10 "xmlns:SOAP-ENV",
value=0x0) at ../../stdsoap2.c:13871
#3  0x00005555555ca19f in soap_out_xsd__anyType (soap=soap@entry=0x7ffff7fba010, tag=0x555555837150 "wst:RequestSecurityToken",
tag@entry=0x0, id=id@entry=0, node=node@entry=0x55555583ebb0,
    type=type@entry=0x0) at ../../dom.c:461
#4  0x00005555555c9ed7 in soap_out_xsd__anyType (soap=soap@entry=0x7ffff7fba010, tag=0x55555583eac0 "SOAP-ENV:Body", tag@entry=0x0,
id=id@entry=0, node=node@entry=0x55555583ea30,
    type=type@entry=0x0) at ../../dom.c:484
#5  0x00005555555d1a26 in soap_wsse_verify_digest (soap=soap@entry=0x7ffff7fba010, alg=alg@entry=19, canonical=canonical@entry=1, id=
<optimized out>,
    hash=hash@entry=0x7fffffffe0b0 "\260~\207\367\060") at ../../plugin/wsseapi.c:4276
#6  0x00005555555d1e54 in soap_wsse_verify_SignedInfo (soap=soap@entry=0x7ffff7fba010) at ../../plugin/wsseapi.c:4161
#7  0x00005555555d2180 in soap_wsse_verify_Signature (soap=soap@entry=0x7ffff7fba010) at ../../plugin/wsseapi.c:3845
#8  0x00005555555d33ac in soap_wsse_preparefinalrecv (soap=0x7ffff7fba010) at ../../plugin/wsseapi.c:7659
#9  0x00005555555c10b8 in soap_end_recv (soap=soap@entry=0x7ffff7fba010) at ../../stdsoap2.c:11512
#10 0x00005555555a54e4 in soap_serve___wst__RequestSecurityToken (soap=soap@entry=0x7ffff7fba010) at soapServer.c:95
#11 0x00005555555a5b0e in soap_serve_request (soap=soap@entry=0x7ffff7fba010) at soapServer.c:62
#12 0x00005555555a5ba0 in soap_serve (soap=0x7ffff7fba010) at soapServer.c:37
#13 0x00005555555af35 in main (argc=<optimized out>, argv=0x7fffffffe448) at wstdemo.c:186
```

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-2020-1187

NEXT REPORT TALOS-2020-1189
