Talos Vulnerability Report

TALOS-2020-1185

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

JANUARY 5, 2021

CVE NUMBER

CVE-2020-13574

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. The KeyInfo element can be used to specifiy certain key and encryption type information. Within the KeyInfo element, a SecurityTokenReference may be used to to reference elements from other parts of the documents. Finally, within this reference element, a KeyIdentifier element may be included. A denial of service condition can occur due to a null pointer dereference if the KeyIdentifier elements does not include a ValueType attribute.

keytype is set here but is never checked to make sure it’s valid.

```
att = soap_att_get(elt, NULL, "ValueType");
keytype = soap_att_get_text(att);
keydata = soap_elt_get_text(elt);
```

soap_att_get_text only checks att but not att->text

```
soap_att_get_text(const struct soap_dom_attribute *att)
{
  if (att)
    return att->text;
  return NULL;
}
```

At this point, keytype is never validated before it is used.

```
      if (!strcmp(keytype, wsse_X509v3URI))
```

Crash Information

```
(gdb) r ns 8080
Starting program: /gsoap-2.8-wsa/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: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  0x00005555555f8ab5 in soap_wsse_verify_EncryptedKey (soap=0x7ffff7fbe010) at ../../plugin/wsseapi.c:5145
#2  0x00005555555fcbf0 in soap_wsse_element_end_in (soap=0x7ffff7fbe010, tag1=0x7ffff7fdb228 "EncryptedKey", tag2=0x5555556048c6
"ds:KeyInfo") at ../../plugin/wsseapi.c:7318
#3  0x00005555555d6512 in soap_element_end_in (soap=0x7ffff7fbe010, tag=0x5555556048c6 "ds:KeyInfo") at ../../stdsoap2.c:14022
#4  0x000055555559ff73 in soap_in_ds__KeyInfoType (soap=0x7ffff7fbe010, tag=0x5555556048c6 "ds:KeyInfo", a=0x555555855080,
type=0x555555603cc0 "") at soapC.c:19442
#5  0x00005555555b61c7 in soap_in_PointerTo_ds__KeyInfo (soap=0x7ffff7fbe010, tag=0x5555556048c6 "ds:KeyInfo", a=0x555555850df8,
type=0x555555603cc0 "") at soapC.c:26085
#6  0x000055555559f506 in soap_in_xenc__EncryptedKeyType (soap=0x7ffff7fbe010, tag=0x555555606990 "xenc:EncryptedKey", a=0x555555850df0,
type=0x5555556047b1 "xenc:EncryptedKeyType")
    at soapC.c:19252
#7  0x00005555555b9844 in soap_in_PointerToxenc__EncryptedKeyType (soap=0x7ffff7fbe010, tag=0x555555606990 "xenc:EncryptedKey",
a=0x555555848060,
    type=0x5555556047b1 "xenc:EncryptedKeyType") at soapC.c:27117
#8  0x000055555559fd8a in soap_in_ds__KeyInfoType (soap=0x7ffff7fbe010, tag=0x5555556048c6 "ds:KeyInfo", a=0x555555848060,
type=0x555555603cc0 "") at soapC.c:19400
#9  0x00005555555b61c7 in soap_in_PointerTo_ds__KeyInfo (soap=0x7ffff7fbe010, tag=0x5555556048c6 "ds:KeyInfo", a=0x555555850b68,
type=0x555555603cc0 "") at soapC.c:26085
#10 0x000055555559f506 in soap_in_xenc__EncryptedKeyType (soap=0x7ffff7fbe010, tag=0x555555606990 "xenc:EncryptedKey", a=0x555555850b60,
type=0x5555556047b1 "xenc:EncryptedKeyType")
    at soapC.c:19252
#11 0x00005555555b9844 in soap_in_PointerToxenc__EncryptedKeyType (soap=0x7ffff7fbe010, tag=0x555555606990 "xenc:EncryptedKey",
a=0x55555582a420,
    type=0x5555556047b1 "xenc:EncryptedKeyType") at soapC.c:27117
#12 0x000055555559fd8a in soap_in_ds__KeyInfoType (soap=0x7ffff7fbe010, tag=0x5555556048c6 "ds:KeyInfo", a=0x55555582a420,
type=0x555555603cc0 "") at soapC.c:19400
#13 0x00005555555b61c7 in soap_in_PointerTo_ds__KeyInfo (soap=0x7ffff7fbe010, tag=0x5555556048c6 "ds:KeyInfo", a=0x555555855148,
type=0x555555603cc0 "") at soapC.c:26085
#14 0x000055555559f506 in soap_in_xenc__EncryptedKeyType (soap=0x7ffff7fbe010, tag=0x555555606990 "xenc:EncryptedKey", a=0x555555855140,
type=0x5555556047b1 "xenc:EncryptedKeyType")
    at soapC.c:19252
#15 0x00005555555b9844 in soap_in_PointerToxenc__EncryptedKeyType (soap=0x7ffff7fbe010, tag=0x555555606990 "xenc:EncryptedKey",
a=0x55555584f608,
    type=0x5555556047b1 "xenc:EncryptedKeyType") at soapC.c:27117
#16 0x000055555557e959 in soap_in__wsse__Security (soap=0x7ffff7fbe010, tag=0x55555560487e "wsse:Security", a=0x55555584f5f0,
type=0x555555603cc0 "") at soapC.c:9498
#17 0x00005555555a8e39 in soap_in_PointerTo_wsse__Security (soap=0x7ffff7fbe010, tag=0x55555560487e "wsse:Security", a=0x55555584f4f0,
type=0x555555603cc0 "") at soapC.c:22092
#18 0x000055555557dba4 in soap_in_SOAP_ENV__Header (soap=0x7ffff7fbe010, tag=0x555555603cb0 "SOAP-ENV:Header", a=0x55555584f4f0, type=0x0)
at soapC.c:9262
#19 0x000055555555dbd4 in soap_getheader (soap=0x7ffff7fbe010) at soapC.c:29
#20 0x00005555555e85a7 in soap_recv_header (soap=0x7ffff7fbe010) at ../../stdsoap2.c:21204
#21 0x00005555555e61d5 in soap_begin_serve (soap=0x7ffff7fbe010) at ../../stdsoap2.c:20487
#22 0x00005555555bb14c in soap_serve (soap=0x7ffff7fbe010) at soapServer.c:32
#23 0x000055555555b405 in main (argc=3, argv=0x7fffffffe4a8) 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

NEXT REPORT

TALOS-2020-1163

TALOS-2020-1186