Talos Vulnerability Report

TALOS-2021-1245

Genivia gSOAP WS-Addressing plugin code execution vulnerability redux

MARCH 24, 2021

CVE NUMBER

CVE-2021-21783

Summary

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

Tested Versions

Genivia gSOAP 2.8.109
Genivia gSOAP 2.8.110

Product URLs

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

CVSSv3 Score

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

CWE

CWE-680 - Integer Overflow to Buffer Overflow

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 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 for providing URI parameters to a number of different parts of both requests and responses. The URIs may include a username and password for the resource in a standard format. http://user:password@somehost.com A buffer overflow vulnerability existing in the parsing of these extra parameters.

While testing a newer version of gSOAP (2.8.110), it was discovered that we were able to reproduce a previously patched vulnerability again. This vulnerability, TALOS-2020-1187, was disclosed to Genivia and patched in an update in October of 2020. Details of the vulnerability remain the same.

Changes were made to soap_decode to check for negative values but unforunately the checks were added comparing size_t types. size_t data types are unsigned integers which can never hold negative values. When the initial size calculation occurs, an unsigned value will wrap around to a very large number resulting in this condition always being true.

```
soap_decode(char *buf, size_t len, const char *val, const char *sep)
{
  const char *s;
  char *t = buf;
  size_t i = len;
  if (!buf || !val || !sep || len == 0)
    return val;
  for (s = val; *s; s++)
    if (*s != ' ' && *s != '\t' && !strchr(sep, *s))
      break;
  if (len > 0)
  {
    if (*s == '"')
    {
      s++;
      while (*s && *s != '"' && i-- > 1)
        *t++ = *s++;
    }
    else
    {
      while (*s && !strchr(sep, *s) && i-- > 1)
      {
        if (*s == '%' && s[1] && s[2])
        {
          *t++ = ((s[1] >= 'A' ? (s[1] & 0x7) + 9 : s[1] - '0') << 4)
                + (s[2] >= 'A' ? (s[2] & 0x7) + 9 : s[2] - '0');
          s += 3;
        }
        else
          *t++ = *s++;
      }
    }
    buf[len - 1] = '\0'; /* appease static checkers that get confused */
  }
  *t = '\0';
  while (*s && !strchr(sep, *s))
    s++;
  return s;
}
```

Timeline

2021-01-22 - Vendor Disclosure
2021-03-24 - Public Release

CREDIT

Discovered by a member of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1226

NEXT REPORT TALOS-2021-1244