Bug 1670254 (CVE-2019-3822) - CVE-2019-3822 curl: NTLMv2 type-3 header stack buffer overflow

Keywords: Security

Status: CLOSED ERRATA

Alias: CVE-2019-3822

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: ~~Red Hat Product Security~~

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: ~~1672905~~ 1674355 1674356

Blocks: 1670258

TreeView+ depends on / blocked

Reported: 2019-01-29 04:18 UTC by Sam Fowler

Modified: 2021-02-16 22:28 UTC (History)

CC List: 29 users (show)

Fixed In Version: curl 7.64.0

Clone Of:

Environment:

Last Closed: 2019-11-06 00:52:00 UTC

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2019:3701	0	None	None	None	2019-11-05 22:06:09 UTC

Sam Fowler 2019-01-29 04:18:42 UTC Description

```
libcurl versions from 7.36.0 to before 7.64.0 are vulnerable
to a stack-based buffer overflow.
```

The function creating an outgoing NTLM type-3 header (`lib/vauth/ntlm.c:Curl_auth_create_ntlm_type3_message()`), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening.

This output data can grow larger than the local buffer if very large "nt response" data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server.

Such a "large value" needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header.

Bug introduced by:

https://github.com/curl/curl/commit/86724581b6c

Sam Fowler 2019-01-29 04:18:44 UTC Comment 1

Acknowledgments:

Name: Daniel Stenberg (the Curl project)
Upstream: Wenxiang Qian (Tencent Blade Team)

Sam Fowler 2019-02-06 07:49:15 UTC Comment 2

External Reference:

https://curl.haxx.se/docs/CVE-2019-3822.html

Upstream Patch:

https://github.com/curl/curl/commit/50c94842

Sam Fowler 2019-02-06 07:49:24 UTC Comment 3

Created curl tracking bugs for this issue:

Affects: fedora-all [~~bug 1672905~~]

Huzaifa S. Sidhpurwala 2019-02-10 06:07:39 UTC Comment 5

Commit 86724581b6c was not backported for rhel-5/6/7 therefore these packages are not affected.

Huzaifa S. Sidhpurwala 2019-02-11 06:12:30 UTC Comment 8

Versions of curl package shipped with Fedora are compiled with StackGuard enabled:

On disassembling the function (using Fedora 26) noticed that the function has the usual stackguard prologue and epilogue:

```
(gdb) disass Curl_auth_create_ntlm_type3_message
Dump of assembler code for function
Curl_auth_create_ntlm_type3_message:
   0x000000000005d820 <+0>:     push   %r15
   0x000000000005d822 <+2>:     push   %r14
   0x000000000005d824 <+4>:     mov    %rdi,%r15
   0x000000000005d827 <+7>:     push   %r13
   0x000000000005d829 <+9>:     push   %r12
   0x000000000005d82b <+11>:    mov    %rdx,%r14
   0x000000000005d82e <+14>:    push   %rbp
   0x000000000005d82f <+15>:    push   %rbx
   0x000000000005d830 <+16>:    mov    %rcx,%rbx
   0x000000000005d833 <+19>:    pxor   %xmm0,%xmm0
   0x000000000005d837 <+23>:    mov    %rsi,%rbp
   0x000000000005d83a <+26>:    sub    $0x8f8,%rsp
   0x000000000005d841 <+33>:    mov    $0x5c,%esi
   0x000000000005d846 <+38>:    mov    %fs:0x28,%rax   <-
notice the stack cookie being pushed on the stack
   0x000000000005d84f <+47>:    mov    %rax,0x8e8(%rsp)

and later in the function (during the exit)

   0x000000000005d95c <+316>:   mov    0x8e8(%rsp),%rbx
   0x000000000005d964 <+324>:   xor    %fs:0x28,%rbx   <-
stack cookie being checked
   0x000000000005d96d <+333>:   jne    0x5defb
<Curl_auth_create_ntlm_type3_message+1755>

Where the jne points to:

   0x000000000005defb <+1755>:  callq  0xb718

Which uses the plt to jump to __stack_chk_fail

This really implies that the function has stackguard correctly working.

It is most likely that the overflow of ntlmbuf will change the stack-cookie and which will trigger a crash during function return and mitigate any chances of code execution.

More details about stackguard is available at:
https://access.redhat.com/blogs/766093/posts/3548631
```

Huzaifa S. Sidhpurwala 2019-02-11 06:42:52 UTC Comment 10

Mitigation:

Turn off NTLM authentication.

~~Eric Christensen~~ 2019-02-18 14:19:01 UTC Comment 11

Statement:

The versions of curl package shipped with Red Hat Enterprise Linux 5, 6, and 7 do not support NTLMv2 type-3 headers, hence they are not affected by this flaw.

errata-xmlrpc 2019-11-05 22:06:08 UTC Comment 14

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2019:3701 https://access.redhat.com/errata/RHSA-2019:3701

Product Security DevOps Team 2019-11-06 00:52:00 UTC Comment 15

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

https://access.redhat.com/security/cve/cve-2019-3822

Note

You need to log in before you can comment on or make changes to this bug.