Bug 28768 (CVE-2022-23218) - Buffer overflow in svcunix_create with long pathnames (CVE-2022-23218)

Status:	RESOLVED FIXED	**Reported:**	2022-01-12 09:40 UTC by Florian Weimer
Alias:	CVE-2022-23218	**Modified:**	2022-01-17 13:07 UTC (History)
		CC List:	5 users (show)
Product:	glibc		
Component:	network (show other bugs)	**See Also:**	~~CVE-2022-23219~~
		Host:	
Version:	2.34	**Target:**	
		Build:	
Importance:	P2 normal	**Last reconfirmed:**	
Target Milestone:	2.35		
Assignee:	Florian Weimer	**Flags:**	fweimer: security+
URL:			
Keywords:			
Depends on:			
Blocks:			

Attachments
Add an attachment (proposed patch, testcase, etc.)

Note

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

Florian Weimer 2022-01-12 09:40:03 UTC Description

This is similar to ~~bug 22542~~, but in different code:

```
SVCXPRT *
svcunix_create (int sock, u_int sendsize, u_int recvsize, char *path)
{
  bool_t madesock = FALSE;
  SVCXPRT *xprt;
  struct unix_rendezvous *r;
  struct sockaddr_un addr;
  socklen_t len = sizeof (struct sockaddr_in);

  if (sock == RPC_ANYSOCK)
    {
      if ((sock = __socket (AF_UNIX, SOCK_STREAM, 0)) < 0)
        {
          perror (_("svc_unix.c - AF_UNIX socket creation problem"));
          return (SVCXPRT *) NULL;
        }
      madesock = TRUE;
    }
  memset (&addr, '\0', sizeof (addr));
  addr.sun_family = AF_UNIX;
  len = strlen (path) + 1;
  memcpy (addr.sun_path, path, len);
  len += sizeof (addr.sun_family);
[…]
```

There is no length check, either.

Florian Weimer 2022-01-17 13:07:48 UTC Comment 1

Fixed for glibc 2.35 via:

commit f545ad4928fa1f27a3075265182b38a4f939a5f7
Author: Florian Weimer <fweimer@redhat.com>
Date: Mon Jan 17 10:21:34 2022 +0100

CVE-2022-23218: Buffer overflow in sunrpc svcunix_create (~~bug 28768~~)

The sunrpc function svcunix_create suffers from a stack-based buffer overflow with overlong pathname arguments.

Reviewed-by: Siddhesh Poyarekar <siddhesh@sourceware.org>

Format For Printing - XML - Clone This Bug - Top of page