

Forum:[Hack Forums](#)

Thread: [ms15-034 exploit to root windows machine](#)

Broomop - August 10, 2015, 10:11 am

ms15-034 exploit to root windows machine anyone know where i can get a script or anything to exploit this i want it bad :D

bonjourmonsieur - August 10, 2015, 10:30 am

Here:

https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/dos/http/ms15_034_ulonglongadd.rb

Annyst - August 10, 2015, 11:39 am

(Aug 10, 2015 10:30 AM)bonjourmonsieur Wrote: [\[CITE\]](#) Here:

github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/dos/http/ms15_034_ulonglongadd.rb

That's only a denial of service exploit.

Broomop - August 10, 2015, 11:45 am

(Aug 10, 2015 10:30 AM)bonjourmonsieur Wrote: [\[CITE\]](#) Here:

https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/dos/http/ms15_034_ulonglongadd.rb yeah thanks i already know this and it works but its possible to do a payload with this exploit supposedly.

bonjourmonsieur - August 10, 2015, 11:46 am

(Aug 10, 2015 11:39 AM)Annyst Wrote: [\[CITE\]](#) That's only a denial of service exploit.

Quote:Microsoft considered the vulnerability as a remote code execution vulnerability. But at this point, no exploit has been made public that executed code. Only DoS exploits are available.

As far as I can tell, there is no RCE vuln weaponized exploit (public). :)

Broomop - August 10, 2015, 5:01 pm

(Aug 10, 2015 11:46 AM)bonjourmonsieur Wrote: [\[CITE\]](#) As far as I can tell, there is no RCE vuln weaponized exploit (public). :)

thats why i want it. ?

Key Punch - August 10, 2015, 6:13 pm

(Aug 10, 2015 05:01 PM)Broomop Wrote: [\[CITE\]](#) thats why i want it. ?

To weaponize it just change...

```
res = send_request_raw(  
  'uri' => uri,  
  'method' => 'GET',  
  'headers' => {  
    'Range' => "bytes=0-#{upper_range}"  
  }  
)
```

to

```
res = send_request_raw(  
  'uri' => uri,  
  'method' => 'GET',  
  'headers' => {  
    'Range' => "bytes=18-#{upper_range}"  
  }  
)
```

In the metasploit module linked above

Broomop - August 16, 2015, 8:21 pm

(Aug 10, 2015 06:13 PM)thebigchicken Wrote: [\[CITE\]](#) To weaponize it just change...

```
res = send_request_raw(  
  'uri' => uri,  
  'method' => 'GET',  
  'headers' => {  
    'Range' => "bytes=0-#{upper_range}"  
  }  
)
```

to

```
res = send_request_raw(  
  'uri' => uri,  
  'method' => 'GET',  
  'headers' => {  
    'Range' => "bytes=18-#{upper_range}"  
  }  
)
```

In the metasploit module linked above

i

want

shell omg man...

dongrat - August 17, 2015, 3:37 am

google search it to find it thats how I found it

Viktory - August 17, 2015, 3:48 am

Just nitpicking but you can't "root" a windows machine.

Broomop - August 20, 2015, 1:32 pm

i want to exploit the machine man... using shell code all these links just show how stupid you all are?

SIM-2198759 - August 20, 2015, 4:03 pm

(Aug 20, 2015 01:32 PM)Broomop Wrote: [\[CITE\]](#) i want to exploit the machine man... using shell code all these links just show how stupid you all are?

You call everyone stupid, yet ms15-034 is not a "root" exploit.

#Skyline - August 21, 2015, 3:42 am

What the fuck, you can't root a windows machine, and it's not a root exploit.

Get real cunt, no ones gonna help you if you call them stupid.

Broomop - September 9, 2018, 8:46 am

Well ok i want to get into the machine. Posh gits.

CyberStrike - September 9, 2018, 9:34 am

(Sep 9, 2018 08:46 AM)Broomop Wrote: [CITE](#) Well ok i want to get into the machine. Posh gits.

Wow 3 years still trying, I must say I respect your determination. Can you maybe update or give us an idea as to all iimportant information? eg target os, network set (LAN/WAN), are you still using metasploit .. I am sure you have more things you would want to add also