

Alrighty so what happens is:

- 1) The Windows Server Service calls a function named CanonicalizePathName on a attacker supplied pathname.
- 2) If this pathname contains something like \AAA\BBB\.\CCC it will try to replace the previous path segment (the one before \.\) with the path segment after the \.\, in other words it will replace 'BBB\.\CCC' with 'CCC', ending up as \AAA\CCC.
- 3) To find the location where the previous segment is located, the loop responsible for this operation searches `_backwards_` for a backslash ('\').
- 4) If you feed the loop a string like '\A\.\.\ABCD', there is a miscalculation where the backwards search for '\' erroneously starts at 1 byte before the first character of the buffer.
- 5) The loop searches backwards until it finds a '\' (unicode) on the stack, and then copies the segment it wants to move back there.
- 6) If you are able to get a backslash on the stack before the stack frame of a child function, you can reliably use the loop's path segment replace to overwrite this stack frame.
- 7) Because you are essentially writing `_below_` your original stack buffer, this is considered a stack `_underflow_` as opposed to a stack overflow.
- 8) A stack frame contains process critical information that controls the flow of execution, overwriting it allows you to redirect the flow of execution into attacker supplied CPU instructions (arbitrary code execution).

Exploits:

Immunity has fully working and reliable exploit code for Windows 2000 and is working on Windows XP SP2, and the other platforms as time progresses. We were the first to put out reliable code for this vulnerability.

Worm concerns:

The last big RPC worms revolved around the DCOM bug (Blaster), and MS06-040 (coincidentally MS06-040 exploited the same buggy function as MS08-067, just a different bug, which means all the security researchers looking at this function in 2006, completely missed this bug).

Because the last big RPC worms caused widespread filtering of port 139/445 by the big ISP's ... and most sane corporate network policies don't allow these ports inbound either ... I don't see this spreading as a big internet worm.

However, on internal networks (big corporate networks, universities, wifi networks) I could see it wreaking havoc.

A combined attack would be feasible, where someone specifically targets someone with a browser exploit delivered over the internet, to then use the MS08-067 bug to automatically scan and compromise any machines on the internal network.

Firewall exceptions:

Windows will have a firewall exception for ports 139/445 if you have file and printer sharing enabled. Something to be aware of.