Sahil Gupta (GlobalComm Security Operations)

To, CEO, GlobalComm

Board of Trustees

4th March, 2019

Provide an executive summary to explain to the CEO and board of trustees the threat of this attack and how it could negatively impact the organization.

The vulnerability exists in most of the versions of windows server, xp and vista. The vulnerability is used to do the stack buffer overflow by sending specially crafted input to the RPC calls. The RPC calls are type of system calls from one area of memory to another. The vulnerability leverages the way two functions in the "Server" service parses pathname in windows RPC protocol. The buffer overflow then led an attacker control the system remotely through CnC server. This vulnerability once exploited, could have critical impact on endpoint and network infrastructure. Some of the impacts could be listed as below:

- Privilege Escalation: The successful exploitation of the vulnerability could enable the remote code execution of arbitrary code from the attacker's machine in the system memory with elevated privileges.
- Denial of service: This could also lead to the system crash or unavailability of the service at the time unsuccessful attack.
- Lateral movement: Since the vulnerability leverages the RPC requests format in netapi.dll, it can also be used to infect other hosts in the network running vulnerable windows version. The infected machines together form a botnet which could be used to perform other critical attacks.

CVE Details: CVE-2008-4250

CVSS Base Score: 10.0 (Highly critical)

Mitigation: Update the systems

Create a technical summary detailing the attack and how it functions to your security operations team

The vulnerability lies in the server service of the RPC protocol in windows system. RPC, Remote procedure call, is used to make system calls from one memory space to another memory space (mostly used in network sharing) as if it is executing in its own local memory. The parameters and other function handlers are managed by files in RPC library.

One such file known as ”netapi.dll” handles the RPC calls in the network sharing hosts via two function calls:

- NetprPathCanonicalize: The function takes in pathname as an input and converts into its canonical name. It does this by converting all slashes into backslashes and omitting any directory traversal sequences. For Example:

  `../../x/y/z will be turned to ../y/z`
- NetprPathCompare: It also calls the above function first in order to compare two pathnames.

The Vulnerability exists in the NetprPathCanonicalize function in such a way when the function parses the string <pathname>, it fails to handle the case when there is no backslash preceding the traversal sequence. Hence it searches for the backslash in system stack buffer. The attacker can fiddle with the stack in such way that it makes the function to copy the string in the buffer which led to overwrite the buffer and make the attacker execute arbitrary code with system privileges.

The attacker uses this vulnerability and send specially crafted packet to some port being used for network sharing utility which then in turn will trigger the function described above. Once the exploit gets successful, it overflows the stack buffer and overwrite the return pointer to execute certain instructions which will then handover the shell to the target machine on the

CnC server of attacker. The shell will be executed with the system privileges as the shell as netapi.dll runs with System privileges by default.

Research methodologies for ways to detect if this exploit is actively being used on the Network

- Nmap is a utility where you can scan multiple hosts on the network for open ports and services running. The configured nmap scan can also let you scan the hosts for this vulnerability. The command which could be used to scan machines for this vulnerability is :

  ```
  nmap -sU --script smb-vuln-ms08-067.nse -p U:137 <host
  ```

  This will identify if the machine has a vulnerability in it or not. If it does, the immediate action of patching the system should follow.
- The another possible impact which machine could suffer could be a denial of service i.e. system crash. So there is a facility in windows in which the user can determine why the system crashed because before system crashes it logs the information and error details. It also saves the memory snapshot as memory dump which could be analysed if there is overwritten stack which is used for this.
- Another way is to analyse the source of the running services on the machine. If cmd.exe is running, we can check the parent process of the file. If this file's parent process is from netapi.dll, we could further investigate to confirm the attack.
- One can also run an antivirus scan to identify and detect well-known malwares and malicious running on the machine, which could be used to exploit the vulnerabilities. Antiviruses like Sophos, comodo, Norton have already built-in detection and removal mechanism.

- Check for registries and memory dumps on the machine to detect any malicious actions.

What malware used this exploit?

Some of the malwares or Trojans that have been known to use this vulnerability for exploitation are mentioned below:

- Conficker.A: This is the first variant of the conficker malware which used this vulnerability to attack systems. It was used to form the botnet. It was discovered in November 2008 and its first biggest known impact on the network services in UK. Some of the symptoms of the infection are account lockout, inaccessible windows updates, ARP flood on network
- Neeris: This is also a worm that used this vulnerability and spreaded through Microsoft messenger. It changes registries to execute autostart feature and to get itself authorized by windows firewall.
- Synigh: It is also a worm which has the ability todeploy the backdoor in the machine and infects IRC server and let the attacker control machine remotely.
- Mocbot and IRCbot: They were discovered in August 2006 and also been used to infect machines to form botnet.

What were some ways to prevent this attack from occurring aside from applying the patch?

Some of the ways to prevent this attack apart from applying the patch is to use Yara or snort rules on your IPS to prevent the malwares which are using this vulnerability in the vicinity. We can also blacklist IPs related to the attacks. We should also block other indicators of compromise that are updated through security researchers.

Another way to prevent the attack is use the prevention software that can detect the worms and Trojans using this vulnerability like Sophos antivirus, McAfee, Norton. We can use other

network tools to apply packet filtering which would analyse the RPC requests being sent by attacker. We should apply encoding on the input level to avoid direct execution of the characters being sent in exploit.

How does the red team for the company use this new information to benefit the company?

Red team is used to test the security efforts taken in the infrastructure weather is it penetrable or not. After applying all the security mechanism for this vulnerability, red team should check whether there is any port open which can be exploited. Red team should ensure that all security mechanism should be in place working fine without any loop hole.

After red team done with all testing, the proper documentation should follow specifying the methodologies and approach taken to penetrate the network. Then, results should be mentioned in the report and should be verified with the blue team wheather they were able to catch the alert or not. Read team should function as the regular activity, it should not be a onetime thing.