CVE ID: CVE-2017-7494
Severity: HIGH & Impact: HIGH
NIC-CERT/2017-05/001v1
Dated: 27-05-2017

NIC-CERT

Advisory for Remote Code Execution Vulnerability in Samba 3.5.0 Onwards

A. Description

Samba is an open source networking software that allows non-Windows operating systems like Linux or macOS to share network folders, files and printers system with Windows operating system.

All versions of Samba from 3.5.0 (released in March 2010) onwards are vulnerable to remote code execution vulnerability. A malicious authenticated samba client, having write access to the samba share, could use this flaw to execute arbitrary code as root. It can upload a shared library to a writable share, and then cause the server to load and execute it.

B. Favorable Conditions

Favorable conditions that make the vulnerable easily exploitable are,

1. Have file- and printer-sharing port 445 reachable
2. Configure shared files to have write privileges
3. Use known or guessable server paths for those files

C. Affected Systems

All Linux/Unix machines especially network storage systems running Samba 3.5.0 or above
Affected software:

Samba Version < 4.6.4
Samba Version < 4.5.10
Samba Version < 4.4.14

Unaffected software:

Samba Version = 4.6.4
Samba Version = 4.5.10
Samba Version = 4.4.14

D. Detection

1. Check the version of Samba running the on the machine with the following command,

   $ smbstatus

2. On RPM-based distributions, the vulnerability can be tested using the following shell script,
   https://email.gov.in/home/syedhasan.mahmood@nic.in/Briefcase/PubShare/samba-vul-checker.sh

E. Mitigation

Any one of the following,

1. SELinux, if enabled, prevents loading of modules from outside of Samba's module directories and therefore blocks the exploit.
2. Mount the file system which is used by Samba for its writable share using "noexec" option.
3. Add the parameter

   nt pipe support = no

   to the [global] section of smb.conf and restart smbd. This prevents clients from accessing any named pipe endpoints. This can disable some expected functionality for Windows clients and may stop sharing of drive on Windows.
4. To mitigate the possibility of exploitation on Samba 4.0.0 or higher before you can perform a full update of the Samba suite, add the following line to the [global] section of the /etc/samba/smb.conf configuration file

   rpc_server:netlogon=disabled

   For the configuration change to take effect, the smbd daemon must be restarted. Note that this mitigation does not work with Samba versions 3.6.x and earlier.

F. Resolution

Patch the systems running the vulnerable versions of Samba. Updates are available for following flavors of Linux,

1. Red Hat Enterprise Linux / Fedora / CentOS / Oracle Enterprise Linux
2. Debian / Ubuntu
3. FreeBSD
4. SUSE

Alternatively, source code patch can also be downloaded from following link,

https://www.samba.org/samba/history/security.html

G. References

1. https://www.samba.org/samba/security/CVE-2017-7494.html
2. https://access.redhat.com/security/cve/CVE-2017-7494
3. https://access.redhat.com/articles/1346913
4. https://github.com/omri9741/cve-2017-7494
5. https://arstechnica.com/security/2017/05/a-wormable-code-execution-bug-has-lurked-in-samba-for-7-years-patch-now/
6. https://securityonline.info/cve-2017-7494-samba-remote-code-execution-vulnerability/
7. https://community.rapid7.com/community/infosec/blog/2017/05/25/patching-cve-2017-7494-in-samba-it-s-the-circle-of-life