BugsBD vulnerability assessment report on Provided VM

Jahid Hossain Sabit

Date
4-jan-2024

Executive Summery

To perform the Vulnerability Assessment of the system, the testing was done in 'Provided VM' by the Authority of BugsBD. Testing was done accordance with information security practices and guidelines of the BugsBD. The objective of the task is to discover flaws and weakness of machine and find vulnerability of the system. Compromise of sensitive system and data by providing details on vulnerabilities and specific remediation guidance.

Test Systems Information:

The test VM has Debian based Linux kernel. The actual version of OS can be 3.2-3.10 but most likely it is 3.7. At first glance the host is locked behind a password and a ssh encryption and there in no telnet (23), http (80), https (443) port is open.

Tools Used for Assessment:

Tool that I used for the Vulnerability Assessment for the System:

- Nmap
- nmapAutomator
- Spiderfoot
- Nessus
- Kali-linux
- Nikto
- Metasploit

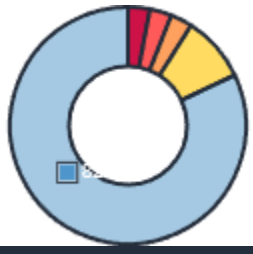
Target system:

Open ports:

Target	Port	Connection	Service	version
192.168.0.9 (VM's ip on my network)	22	TCP	ssh	OpenSSH 6.0p1 protocol 2.0
	111	TCP	rpcbind	2-4(RPC#100000)
	8080	TCP	http-proxy, ftp	proFTPD 1.3.3c
	54289	TCP	unknown	
	111	UDP	rpcbind	2-4(RPC#100000)
	123	UDP	NTP	NTP v4

Findings Summery:

Critical	High	Medium	Low	info
1	1	1	3	33



Critical: Unix Operating System Unsupported Version

Description:
According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution:
Upgrade to a version of the Unix operating system that is currently supported.

CVSS v3 Base Score:
10.0

High: ProFTPD Compromised Source Packages Trojaned Distribution

Description:
The remote host is using ProFTPD, a free FTP server for Unix and Linux.

The version of ProFTPD installed on the remote host has been compiled with a backdoor in 'src/help.c', apparently related to a compromise of the main distribution server for the ProFTPD project on the 28th of November 2010 around 20:00 UTC and not addressed until the 2nd of December 2010.
By sending a special HELP command, an unauthenticated, remote attacker can gain a shell and execute arbitrary commands with system privileges.

Solution:
Reinstall the host from known, good sources.

CVSS v3.0 Base Score:
8.8

Medium: SSH Weak Algorithms Supported

Description:
By Nessus, it has been detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

Solution:
Contact the vendor or consult product documentation to remove the weak ciphers.

CVSS v3.0 Base Score:
4.3

Low: SSH Server CBC Mode Ciphers Enabled

Description
The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.
Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution
Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

CVSS v3.0 Base Score:
3.7

Low: SSH Weak Key Exchange Algorithms Enabled

Description
The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Solution
Contact the vendor or consult product documentation to disable the weak algorithms.

CVSS v3.0 Base Score:
3.7

Low: SSH Weak MAC Algorithms Enabled

Description
The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Solution
Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

CVSS v3.0 Base Score:
Not available but CVSS v2 indicates 2.6

Exploits can be Used at Current settings:

Port :22

- SSV:92672 7.8 https://vulners.com/seebug/SSV:92672
- EDB-ID:41278 7.8 https://vulners.com/exploitdb/EDB-ID:41278
- 1337DAY-ID-26918 7.8 https://vulners.com/zdt/1337DAY-ID-26918
- 1337DAY-ID-26888 7.8 https://vulners.com/zdt/1337DAY-ID-26888
- SSV:61450 7.5 https://vulners.com/seebug/SSV:61450
- EDB-ID:42271 7.5 https://vulners.com/exploitdb/EDB-ID:42271
- EDB-ID:47803 7.2 https://vulners.com/exploitdb/EDB-ID:47803
- EDB-ID:47780 7.2 https://vulners.com/exploitdb/EDB-ID:47780
- 1337DAY-ID-39095 7.2 https://vulners.com/zdt/1337DAY-ID-39095
- PACKETSTORM:140944 0.0 https://vulners.com/packetstorm/PACKETSTORM:140944

Port:111
Not available

Port:8080

- SAINT:FD1752E124A72FD3A26EEB9B315E8382 10.0
  https://vulners.com/saint/SAINT:FD1752E124A72FD3A26EEB9B315E8382
- SAINT:950EB68D408A40399926A4CCAD3CC62E 10.0
  https://vulners.com/saint/SAINT:950EB68D408A40399926A4CCAD3CC62E
- SAINT:63FB77B9136D48259E4F0D4CDA35E95710.0
  https://vulners.com/saint/SAINT:63FB77B9136D48259E4F0D4CDA35E957

- SAINT:1B08F4664C428B180EEC9617B41D9A2C 10.0 https://vulners.com/saint/SAINT:1B08F4664C428B180EEC9617B41D9A2C
- PROFTPD_MOD_COPY 10.0 https://vulners.com/canvas/PROFTPD_MOD_COPY
- PACKETSTORM:162777 10.0 https://vulners.com/packetstorm/PACKETSTORM:162777
- PACKETSTORM:132218 10.0 https://vulners.com/packetstorm/PACKETSTORM:132218
- PACKETSTORM:131567 10.0 https://vulners.com/packetstorm/PACKETSTORM:131567
- PACKETSTORM:131555 10.0 https://vulners.com/packetstorm/PACKETSTORM:131555
- PACKETSTORM:131505 10.0 https://vulners.com/packetstorm/PACKETSTORM:131505
- EDB-ID:49908 10.0 https://vulners.com/exploitdb/EDB-ID:49908
- 1337DAY-ID-36298 10.0 https://vulners.com/zdt/1337DAY-ID-36298
- 1337DAY-ID-23720 10.0 https://vulners.com/zdt/1337DAY-ID-23720
- 1337DAY-ID-23544 10.0 https://vulners.com/zdt/1337DAY-ID-23544
- ftp-proftpd-backdoor: This installation has been backdoored.