Werick Passon

https://github.com/naevox/

https://www.linkedin.com/in/werick-p-b9b90493/

Index:

page 1 - Intro

page 1 - Scope

page 1 - Identified Vulnerabilities

page 1 > Credential backup accessible externally (High)

page 2 > BIND's GSSAPI security policy negotiation buffer overflow vuln (Medium)

page 2 > Server information disclosure (Low)

page 3 > Out of date SSL certificate (Low)

page 3 > Outdated DNS service, vulnerable to multiple Denial Of Service (Low)

page 3 > Port commonly used in DDoS open to external internet (Low)

page 4 - Conclusion

**Intro:**

This penetration test was carried out by Werick Passon. It was carried out for 7 days. A High severity vulnerability where someone has left a password backup file within the web directory file hierarchy. In addition to that an information disclosure web directory leads to server base system information disclosure. Along with a new CVE to patch against and 3 Low findings which may need to be addressed some time in the near future.

**Scope:**

- 10.10.10.10

**Identified Vulnerabilities:**

The following sections list vulnerabilities. The findings are listed in chronological order and not by their degree of severity. The severity is given in brackets following the title heading. Each bug is given a unique identifier for the purpose of future reference and follow-up.

**Credential backup accessible externally (High)**

Description:

Password backup accessible for users without authentication being required to reach it. This information can be reached by simply typing the bellow URL into a browser you are able to see user credentials and password hashes for them. Using an identifier we find it is a MD5 hash sum. Using hashcat we recover the password for user1 and found the hash for user2 is available in hashes.com.

PoC:

curl 10.10.10.10:80/backup/pass.txt

===

user1:9f9d51bc70ef21ca5c14f307980a29d8 - bob

user2:9f9d51bc70ef21ca5c14f307980a29d8 – available on hashes.com

root:9f9d51bc70ef21ca5c14f307980a29d8

- The passwords file

- The fact they had the hash on hashes.com

Mitigation:

Remove this file from the web directory hierarchy.

**BIND's GSSAPI security policy negotiation buffer overflow vulnerability (Medium)**

Description:

The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error within the SPNEGO implementation in the GSS-TSIG extension. A remote attacker can send a specially crafted DNS request to the server, trigger memory corruption and execute arbitrary code on the target system.

Successful exploitation of this vulnerability may result in complete compromise of vulnerable system. CVE-2020-8625.

PoC: Not available.

Mitigation:

Ensure server is patched against cve-2020-8625

Reference:

https://nvd.nist.gov/vuln/detail/CVE-2020-8625

**Server information disclosure (Low)**

Description:

It is possible to obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

PoC:

curl http://10.10.10.10:80/server-status/

DISTRIB\_ID=Ubuntu

DISTRIB\_RELEASE=16.04

DISTRIB\_CODENAME=xenial

DISTRIB\_DESCRIPTION="Ubuntu 16.04.6 LTS"

message here: Linux interview-system-2 4.4.0-166-generic #195-Ubuntu SMP Tue Oct 1 09:36:25 UTC 2019 i686 i686 i686 GNU/Linux

linux-gate.so.1 => (0xb7fda000)

libselinux.so.1 => /lib/i386-linux-gnu/libselinux.so.1 (0xb7faa000)

libc.so.6 => /lib/i386-linux-gnu/libc.so.6 (0xb7df3000)

libpcre.so.3 => /lib/i386-linux-gnu/libpcre.so.3 (0xb7d7e000)

libdl.so.2 => /lib/i386-linux-gnu/libdl.so.2 (0xb7d79000)

/lib/ld-linux.so.2 (0xb7fdb000)

libpthread.so.0 => /lib/i386-linux-gnu/libpthread.so.0 (0xb7d5c000)

linux-gate.so.1 => (0xb7fda000)

libselinux.so.1 => /lib/i386-linux-gnu/libselinux.so.1 (0xb7faa000)

libc.so.6 => /lib/i386-linux-gnu/libc.so.6 (0xb7df3000)

libpcre.so.3 => /lib/i386-linux-gnu/libpcre.so.3 (0xb7d7e000)

libdl.so.2 => /lib/i386-linux-gnu/libdl.so.2 (0xb7d79000)

/lib/ld-linux.so.2 (0xb7fdb000)

libpthread.so.0 => /lib/i386-linux-gnu/libpthread.so.0 (0xb7d5c000)

Mitigation:

If required, update Apache's configuration file(s) to either disable mod\_status or ensure that access is limited to valid users / hosts.

Reference:

https://www.tenable.com/plugins/was/98225

**Out of date SSL certificate (Low)**

Description:

When using an expired certificate, you risk your encryption and mutual authentication. As a result, both your website and users are susceptible to attacks and viruses. For example, a hacker can take advantage of a website with an expired SSL certificate and create a fake website identical to it.

PoC:

nmap -A -p 443 10.10.10.10

443/tcp open ssl/http nginx 1.10.3 (Ubuntu)

| Not valid before: 2019-11-09T14:07:05

|\_Not valid after: 2020-11-08T14:07:05

Mitigation:

Update SSL certificate.

References:

https://www.venafi.com/education-center/ssl/fix-expired-certificates

**Outdated DNS service, vulnerable to multiple Denial Of Service (Low)**

Description:

13 available DoS vulnerabilities available for ‘ISC BIND 9.10.3-P4’ which will cause downtime if executed against the machine during normal run time.

PoC:

https://www.cybersecurity-help.cz/vdb/isc/isc\_bind/9.10.3-p4/

Mitigation:

Patch DNS server to latests patches available.

Reference:

https://www.cybersecurity-help.cz/vdb/isc/isc\_bind/9.10.3-p4/

**Port commonly used in DDoS open to external internet (Low)**

Description:

It is a very old protocol which can be exploited to execute amplified attacks. A CharGEN amplification attack is carried out by sending small packets carrying a spoofed IP of the target to internet enabled devices running CharGEN. These spoofed requests to such devices are then used to send UDP floods as responses from these devices to the target.

PoC:

nmap -A -p 19 10.10.10.10

19/tcp open chargen Linux chargen

Mitigation:

Close port with firewall, if not possible

Keep host for internal use only

Reference:

https://javapipe.com/blog/ddos-types/

**Conclusion:**

passwords.txt backup file retrievable by anyone who has access to the server. The fact that this can be remote exploited by an unauthenticated user makes this a high impact issue and not critical due to the credentials not being usable with the SSH service due to it requiring a public key to work. Another thing which was notable was information disclosure when accessing ‘/server-status/’ directory as this can aid in narrow the enumeration requirement and aids in privilege escalation if remote code execution has already been achieved. These along with informational level reportable findings on out of date SSL which may allow for MiTM attacks.