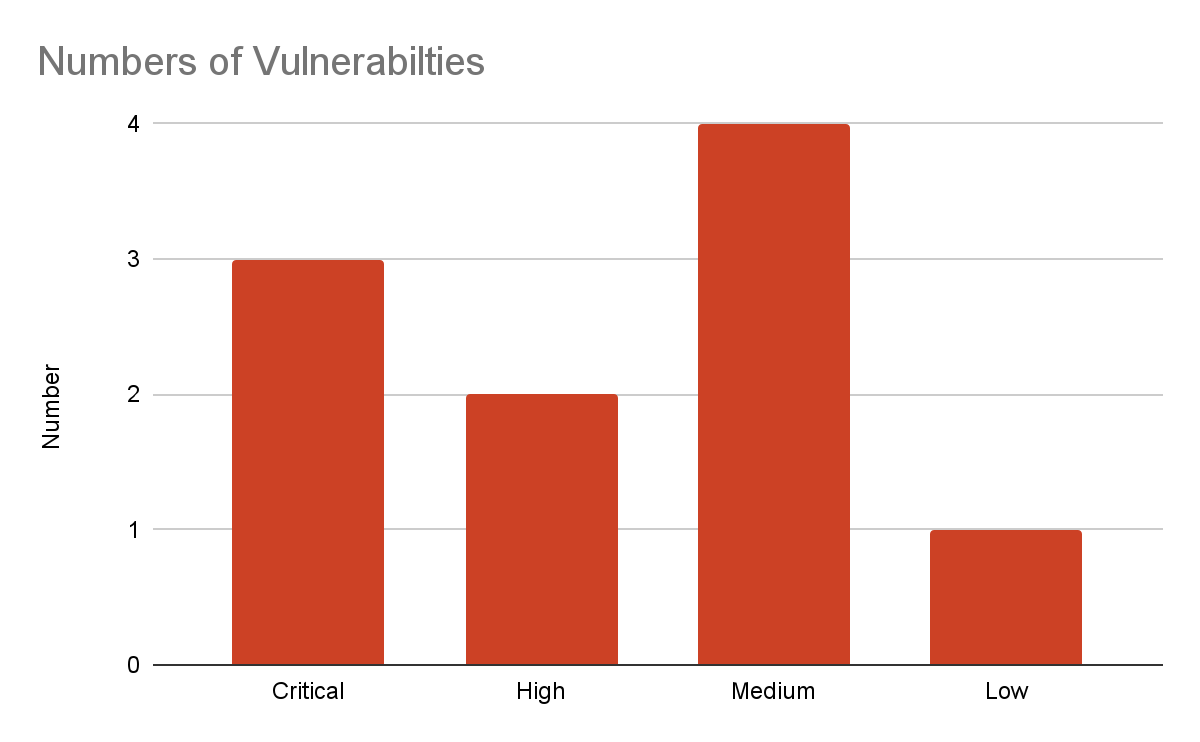
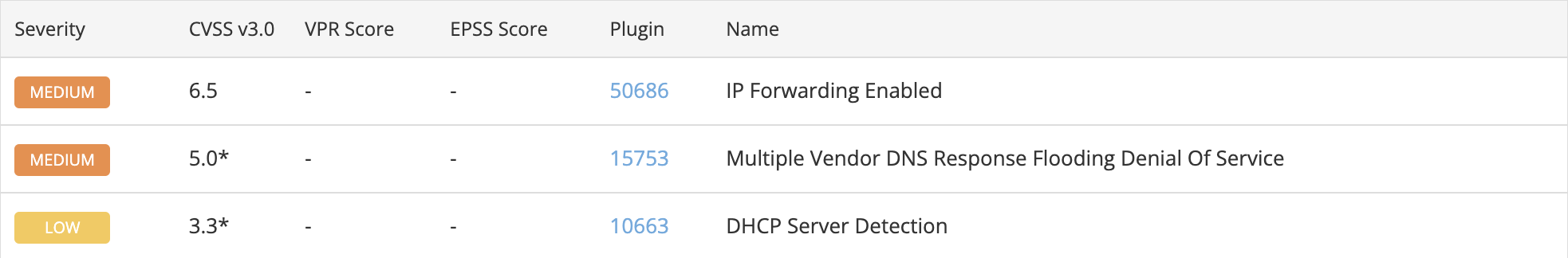
# 1. Analyzation

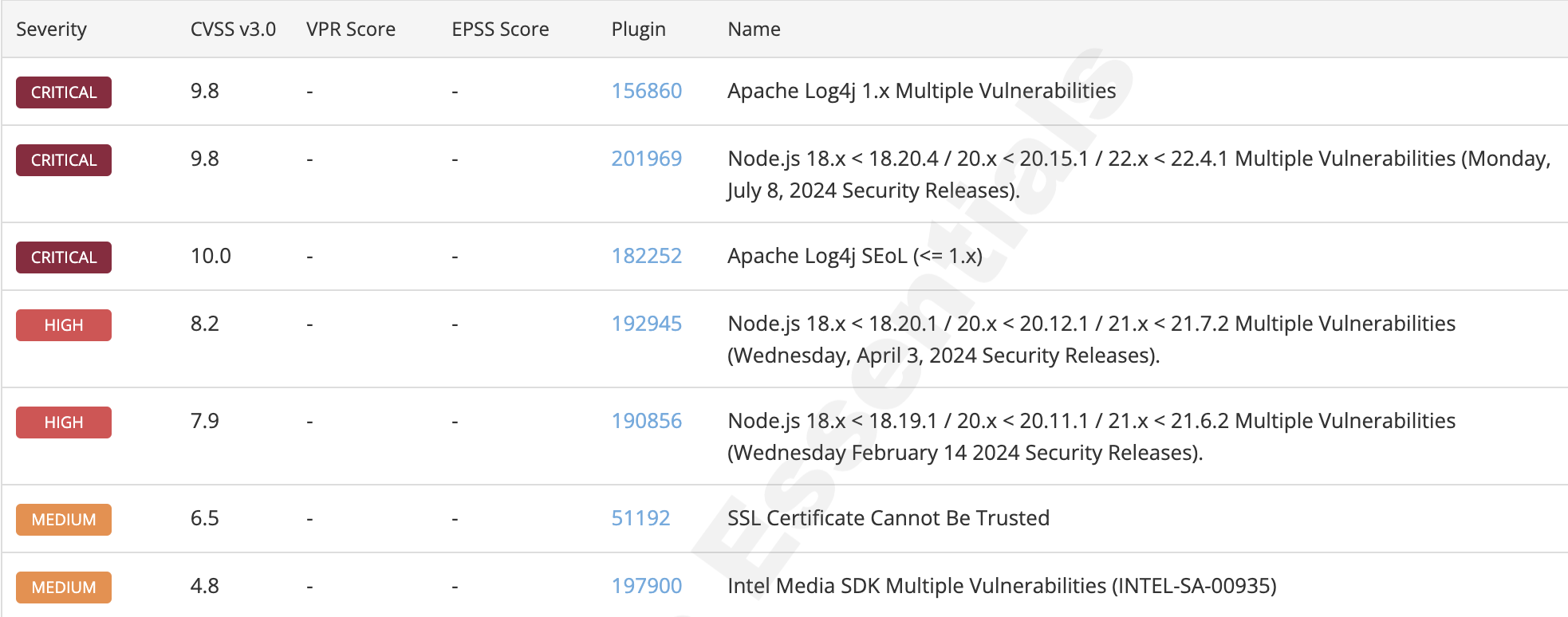
## 1. Scan result

* **Total number of vulnerabilities : 10**
* Critical severity : 3
* High severity : 2
* Medium severity : 4
* Low severity : 1









## 2. Key issues in result

* Outdated software
* Unactivated firewall
* Misconfiguration firewall rules

# 

# 2. List the top priorities by CVSS

## 1. Apache

### Cause

An outdated version of Apache with known vulnerabilities was downloaded.

### Impact

* Remote code execution can be performed through SocketServer.
* Sensitive information may be leaked through log messages.
* Unintended SQL queries may be executed.

### Solution

Update to the latest version of Apache.

## 2. Node.js

### Cause

A version of Node.js with known vulnerabilities was downloaded.

### Impact

* The file owner permissions can be changed when using the --allow-fs-write flag.
* Network import restrictions can be bypassed, posing a threat to the server.

### Solution

Upgrade Node.js to version 18.20.4 / 20.15.1 / 22.4.1, or later.

## 3. IP Forwarding Enabled

* Cause

Resetting firewall rules also removed traffic filtering rules.

### Impact

An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

### Solution

Run the following command to disable IP forwarding:

echo 0 > /proc/sys/net/ipv4/ip\_forward

## 4. SSL Certificate Cannot Be Trusted

### Cause

A vulnerability was detected in the SSL certificate present in the OS, indicating it is not trusted.

### Impact

* HTTPS communication is not guaranteed, making the system vulnerable to man-in-the-middle (MITM) attacks.
* Increased risk of connecting to malicious software updates, phishing sites, or fake servers.

### Solution

Regenerate proper SSL certificates.

## 5. Multiple Vendor DNS Response Flooding Denial Of Service

### Cause

The firewall controlling network traffic was disabled.

### Impact

An attacker could exploit this vulnerability by spoofing a DNS packet so that it appears to come from 127.0.0.1 and make the remote DNS server enter into an infinite loop, therefore denying service to legitimate users.

### Solution

* Create firewall rules to block attackers generating excessive traffic.
* Upgrade the DNS software to the latest version.

## 

## 6. Intel Media SDK Multiple Vulnerabilities (INTEL-SA-00935)

### Cause

A vulnerability was detected in the video processing library included by default in the OS.

### Impact

* Improper input validation in Intel Media SDK software all versions may allow an authenticated user to potentially enable denial of service via local access.
* Improper buffer restrictions in Intel Media SDK all versions may allow an authenticated user to potentially enable escalation of privilege via local access.
* Out-of-bounds read in Intel Media SDK and some Intel oneVPL software before version 23.3.5 may allow an authenticated user to potentially enable escalation of privilege via local access.
* Out-of-bounds write in Intel Media SDK all versions and some Intel oneVPL software before version 23.3.5 may allow an authenticated user to potentially enable escalation of privilege via local access.
* Improper buffer restrictions in Intel Media SDK software all versions may allow an authenticated user to potentially enable denial of service via local access.

### Solution

Since Intel has discontinued support, you should discontinue use of the software or remove it.

## 7. DHCP Server Detection

* Cause

The firewall controlling network traffic was disabled.

### Impact

A local attacker may use DHCP to become intimately familiar with the associated network because some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on.

### Solution

* Reconfigure firewall rules to block suspicious IPs.
* Update the DHCP software to the latest version.