**LIST OF VULNERABILITIES OF USED DEPENDENCIES - THEIR SECURITY FAILURES AND PREVENTIVE MEASURES**

**1. HDFS V2.4.0-**

* **CVE-2018-6185: Apache Airflow HDFS Provider**
  + Description: Incorrect documentation pointed users to an incorrect pip package, which could potentially be claimed by an attacker to execute malicious code during installation.
  + Severity: 7.8 (HIGH)
  + Recommendations:
    - Upgrade to version 4.1.1 or later, where the Airflow team has fixed the issue.
* **CVE-2016-5001: Apache Hadoop**
  + Description: Information disclosure vulnerability in the short-circuit reads feature of HDFS, where a local user on an HDFS DataNode may craft a block token that grants unauthorized read access to random files.
  + Severity: 5.5 (MEDIUM)
  + Recommendations:
    - Upgrade to a version that includes a fix for this vulnerability.
* **CVE-2017-3162: Apache Hadoop**
  + Description: HDFS clients interact with a servlet on the DataNode to browse the HDFS namespace. The NameNode is provided as a query parameter that is not validated.
  + Severity: 7.3 (HIGH)
  + Recommendations:
    - Upgrade to a version that includes a fix for this vulnerability.
* **CVE-2017-3161: Apache Hadoop**
  + Description: The HDFS web UI is vulnerable to a cross-site scripting (XSS) attack through an unescaped query parameter.
  + Severity: 6.1 (MEDIUM)
  + Recommendations:
    - Upgrade to a version that includes a fix for this vulnerability.
* **CVE-2014-0229: Apache Hadoop**
  + Description: Hadoop does not check authorization for certain HDFS admin commands, allowing remote authenticated users to cause a denial of service or perform unnecessary operations.
  + Severity: 6.5 (MEDIUM)
  + Recommendations:
    - Upgrade to a version that includes a fix for this vulnerability.
* **CVE-2016-5393: Apache Hadoop**
  + Description: A remote user who can authenticate with the HDFS NameNode can possibly run arbitrary commands with the same privileges as the HDFS service.
  + Severity: 8.8 (HIGH)
  + Recommendations:
    - Upgrade to a version that includes a fix for this vulnerability.
* **CVE-2015-1889: IBM InfoSphere BigInsights**
  + Description: The Big SQL component allows remote authenticated users to bypass intended HDFS data-access restrictions.
  + Severity: Not specified
  + Recommendations:
    - Upgrade to a version that includes a fix for this vulnerability.

**2. JWT-GO v3.2.0 -**

* **CVE-2020-26160** 
  + Description: jwt-go before 4.0.0-preview1 allows attackers to bypass intended access restrictions in situations with **[]string{}** for **m["aud"]** (which is allowed by the specification). Because the type assertion fails, **""** is the value of **aud**. This is a security problem if the JWT token is presented to a service that lacks its own audience check.
  + Severity: Not specified
  + Recommendations:
    - Upgrade to version 4.0.0-preview1 or later, where the issue has been addressed.

**Preventive Measures:**

* Regularly update dependencies: Keep dependencies up-to-date to benefit from the latest security fixes.
* Monitor security mailing lists: Subscribe to security mailing lists for the libraries you use to stay informed about the latest vulnerabilities.
* Use vulnerability scanning tools: Employ automated tools to scan your dependencies for known vulnerabilities.
* Follow security best practices: Implement security best practices for your application and infrastructure.

**3. GO Cryptography -**

* **CVE-2022-27191: golang.org/x/crypto/ssh**
  + Description: The golang.org/x/crypto/ssh package before 0.0.0-20220314234659-1baeb1ce4c0b for Go allows an attacker to crash a server in certain circumstances involving AddHostKey.
  + Severity: Not specified
  + Recommendations:
    - Upgrade to version 0.0.0-20220314234659-1baeb1ce4c0b or later, where the issue has been addressed.
* **CVE-2021-43565: golang.org/x/crypto/ssh**
  + Description: The x/crypto/ssh package before 0.0.0-20211202192323-5770296d904e of golang.org/x/crypto allows an attacker to panic an SSH server.
  + Severity: Not specified
  + Recommendations:
    - Upgrade to version 0.0.0-20211202192323-5770296d904e or later, where the issue has been addressed.
* **CVE-2020-9283: golang.org/x/crypto**
  + Description: golang.org/x/crypto before v0.0.0-20200220183623-bac4c82f6975 for Go allows a panic during signature verification in the golang.org/x/crypto/ssh package. A client can attack an SSH server that accepts public keys. Also, a server can attack any SSH client.
  + Severity: Not specified
  + Recommendations:
    - Upgrade to version v0.0.0-20200220183623-bac4c82f6975 or later, where the issue has been addressed.
* **CVE-2017-3204: golang.org/x/crypto/ssh**
  + Description: The Go SSH library (x/crypto/ssh) by default does not verify host keys, facilitating man-in-the-middle attacks. Default behavior changed in commit e4e2799 to require explicitly registering a hostkey verification mechanism.
  + Severity: Not specified
  + Recommendations:
    - Upgrade to a version that includes a fix for this vulnerability.

**Preventive Measures:**

* Regularly update dependencies: Keep dependencies up-to-date to benefit from the latest security fixes.
* Monitor security mailing lists: Subscribe to security mailing lists for the libraries you use to stay informed about the latest vulnerabilities.
* Use vulnerability scanning tools: Employ automated tools to scan your dependencies for known vulnerabilities.
* Follow security best practices: Implement security best practices for your application and infrastructure, such as verifying host keys explicitly in SSH connections.

**4. ANGULAR v16-**

* **CVE-2023-30589: llhttp parser in Node v20.2.0**
  + Description: The llhttp parser in the http module in Node v20.2.0 does not strictly use the CRLF sequence to delimit HTTP requests, leading to HTTP Request Smuggling (HRS).
  + Severity: Not specified
  + Recommendations:
    - Upgrade to a version of Node.js that includes a fix for this vulnerability.
* **CVE-2023-30588: crypto.X509Certificate() API in Node.js**
  + Description: When an invalid public key is used to create an x509 certificate using the crypto.X509Certificate() API, a non-expect termination occurs, making it susceptible to DoS attacks.
  + Severity: Not specified
  + Recommendations:
    - Upgrade to a version of Node.js that includes a fix for this vulnerability.
* **CVE-2023-30581: Use of proto in process.mainModule.proto.require()**
  + Description: The use of **proto** in process.mainModule.**proto**.require() can bypass the policy mechanism and require modules outside of the policy.json definition.
  + Severity: Not specified
  + Recommendations:
    - Upgrade to a version of Node.js that includes a fix for this vulnerability.
* **CVE-2022-25869: Cross-site Scripting (XSS) in Angular**
  + Description: All versions of package angular are vulnerable to XSS due to insecure page caching in the Internet Explorer browser.
  + Severity: Not specified
  + Recommendations:
    - Implement proper input validation and output encoding to prevent XSS attacks.
    - Consider using Content Security Policy (CSP) headers to mitigate XSS vulnerabilities.
* **CVE-2022-25844: Regular Expression Denial of Service (ReDoS) in Angular**
  + Description: The package angular after 1.7.0 are vulnerable to ReDoS by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER\_FORMATS.PATTERNS[1].posPre with a very high value.
  + Severity: Not specified
  + Recommendations:
    - Upgrade to a version of Angular that is not vulnerable to this issue.
    - Avoid using deprecated and unmaintained packages.

**Preventive Measures:**

* Regularly update dependencies: Keep dependencies up-to-date to benefit from the latest security fixes.
* Implement proper input validation and output encoding to prevent XSS attacks.
* Use Content Security Policy (CSP) headers to mitigate XSS vulnerabilities.
* Avoid using deprecated and unmaintained packages.
* Follow best practices and guidelines for secure coding.