PDF Export for report 2515855

Information Disclosure on https://version.hylatest.com

State	New
Reported by	Mostafa (max0a)
Reported to	Assurant (assurant)
Submitted at	2024-05-22T15:43:29.005Z (ISO-8601)
Asset	https://version.hylatest.com/ (URL)
References	
Weakness	Information Disclosure
Severity	Medium (4.0 ~ 6.9)
CVE IDs	

Summary:

- Vulnerability Type: Information Disclosure
- Vulnerability Location : https://version.hylatest.com/appsce.yml

During a security assessment of the web application https://version.hylatest.com , I discovered an information disclosure vulnerability that exposes sensitive system information. The vulnerability is caused by the exposure of a configuration file that contains details about the system's architecture, operating system, and file system layout

Steps To Reproduce:

- Visit This Domain https://version.hylatest.com/
- Add End Point /appsce.yml
- Wiil download This FIle
- The vulnerable endpoint returns the following response :
- ```
  version: 0.0
  os: linux
  files:
  source: /
  destination: /var/www/html/
  hooks:
  ApplicationStop:
  location: scripts/appstop.sh
  timeout: 6000
  runas: ubuntu
  BeforeInstall:
  location: scripts/beforeinstall.sh
  timeout: 300
  runas: ubuntu
  AfterInstall:
  location: scripts/afterinstall.sh
  timeout: 6000 ```
  ```

This response reveals the following sensitive information:

- The operating system used by the server is Linux.
- The file system layout, including the source and destination directories.
- The existence of scripts and their locations, including appstop.sh, beforeinstall.sh, and afterinstall.sh.
- The user account used to run these scripts, which is ubuntu.
- The timeout values for each script.

To remediate this vulnerability, I recommend the following:

- Restrict access to the configuration file to prevent unauthorized disclosure of sensitive information.
- Implement proper access controls and authentication mechanisms to ensure that only authorized personnel can access the file.
- Review the scripts and their functionality to ensure they are secure and do not introduce additional vulnerabilities.
- Consider implementing a Web Application Firewall (WAF) to detect and prevent similar information disclosure vulnerabilities.
  ```

Impact

This information disclosure vulnerability can have significant implications for the security of the web application. An attacker can use this information to:

- Identify potential vulnerabilities in the Linux operating system or related software.
- Map the file system layout to identify potential entry points for attacks.
- Analyze the scripts and their functionality to identify potential weaknesses or backdoors.
- Use the revealed user account information to launch targeted attacks, such as password guessing or privilege escalation