**Trivy is an open-source vulnerability scanner specifically designed for containers and container images. It's primarily used to scan container images for security vulnerabilities. Trivy scans container images and provides detailed reports on any vulnerabilities found, along with severity levels and remediation suggestions.**

**Use cases for Trivy include:**

**Container Security: Trivy is widely used by DevOps teams and security professionals to ensure the security of containerized applications. By scanning container images during the build and deployment process, teams can identify and fix vulnerabilities before they are deployed into production environments.**

**Continuous Integration/Continuous Deployment (CI/CD): Trivy can be integrated into CI/CD pipelines to automate vulnerability scanning as part of the software development lifecycle. This ensures that container images are continuously scanned for vulnerabilities as they are built and deployed, helping to maintain a high level of security throughout the development process.**

**Security Audits: Organizations can use Trivy to conduct security audits of their container images, identifying any vulnerabilities that may exist within their containerized applications. This helps organizations proactively address security issues and minimize the risk of potential breaches.**

**Compliance Requirements: Trivy can assist organizations in meeting compliance requirements by ensuring that container images meet security standards and regulations. By regularly scanning container images for vulnerabilities, organizations can demonstrate their commitment to maintaining a secure environment for their applications and data.**

**Overall, Trivy plays a crucial role in securing containerized environments by providing comprehensive vulnerability scanning capabilities and helping organizations identify and remediate security risks in their container images.**

**How to Install Trivy :**

[**https://aquasecurity.github.io/trivy/v0.18.3/installation/**](https://aquasecurity.github.io/trivy/v0.18.3/installation/) **- The Given Link is going to help you to install Trivy in different platforms.**

**# Scan a container image**

**$ trivy image python:3.4-alpine**

**# Scan a container image from a tar archive**

**$ trivy image --input ruby-3.1.tar**

**# Scan local filesystem**

**$ trivy fs .**

**# Run in server mode**

**$ trivy server**

**Scanning Commands**

**aws [EXPERIMENTAL] Scan AWS account**

**config Scan config files for misconfigurations**

**filesystem Scan local filesystem**

**image Scan a container image**

**kubernetes [EXPERIMENTAL] Scan kubernetes cluster**

**repository Scan a repository**

**rootfs Scan rootfs**

**sbom Scan SBOM for vulnerabilities and licenses**

**vm [EXPERIMENTAL] Scan a virtual machine image**

**Management Commands**

**module Manage modules**

**plugin Manage plugins**

**Utility Commands**

**completion Generate the autocompletion script for the specified shell**

**convert Convert Trivy JSON report into a different format**

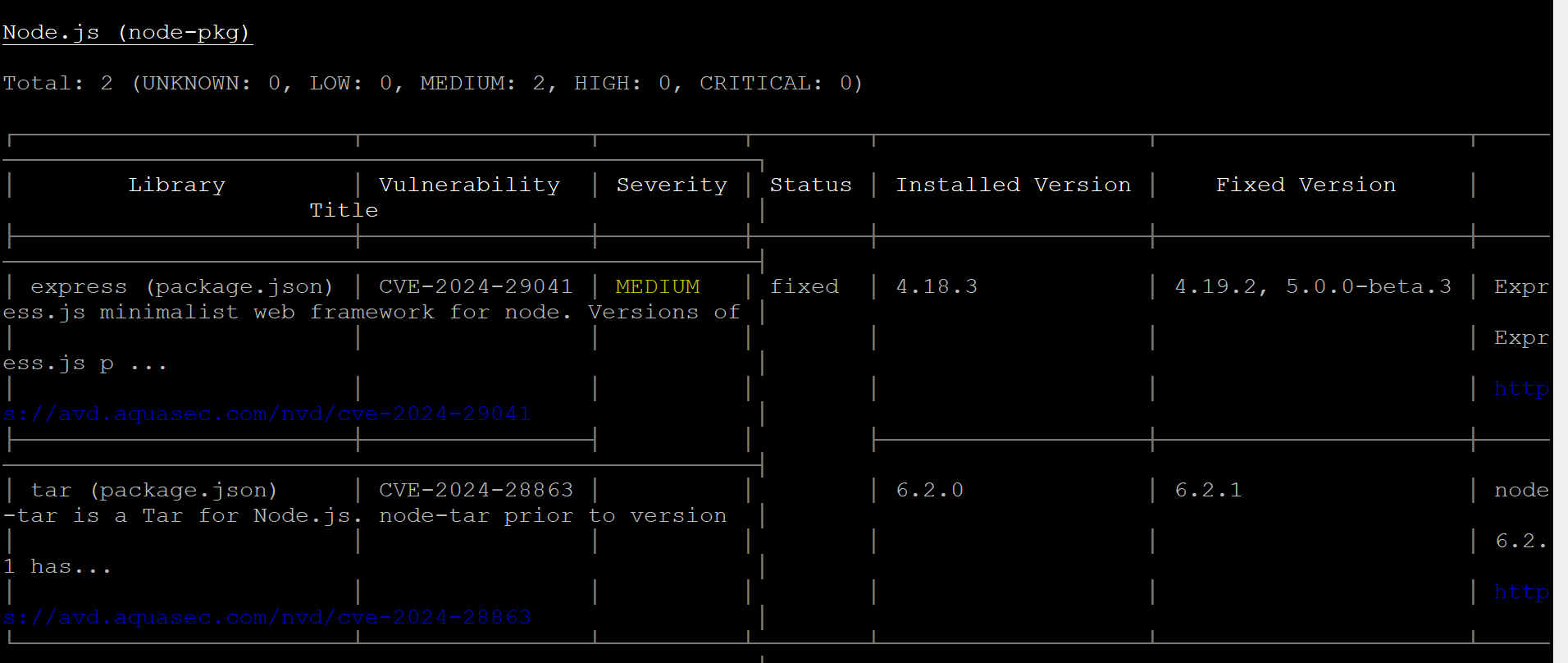
**help Help about any command**

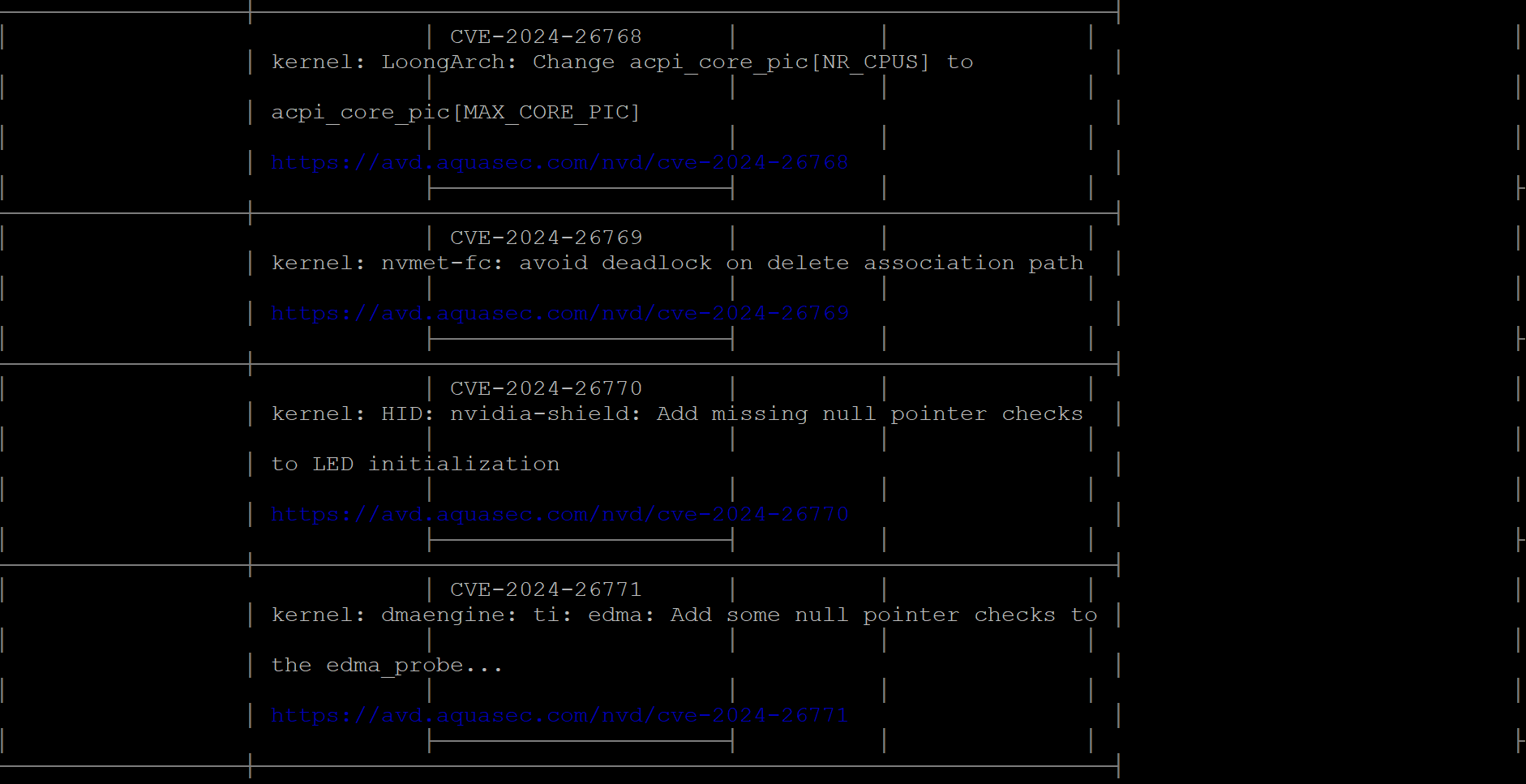
**server Server mode**

**version Print the version**

**Example :**

**Trivy Image muralisocial123/node-example-app:latest**

****

****