Simple Fixes and Mitigations for Identified Vulnerabilities

1. High Severity Vulnerabilities (Node.js Multiple Vulnerabilities)

All the high-severity vulnerabilities related to Node.js stem from using outdated versions. The most direct and effective fix is to update Node.js.

Vulnerabilities Covered:

- Plugin ID 152945
- Plugin ID 174404
- Plugin ID 182366
- Plugin ID 181530
- Plugin ID 175655

Simple Fix/Mitigation:

- Identify Current Node.js Version: Run `node -v` in the terminal.
- Upgrade using Node Version Manager (NVM):
  - nvm install --lts
  - nvm use --lts
  - nvm uninstall <old_version>
- Upgrade using package manager:
  Debian/Ubuntu: sudo apt update && sudo apt upgrade nodejs
  CentOS/RHEL: sudo yum update nodejs or dnf update nodejs
  macOS: brew update && brew upgrade node
  Windows: Download the installer from https://nodejs.org/en/download/
- Verify upgrade using `node -v`

General Mitigation:

- Keep dependencies updated (npm update / yarn upgrade)

- Run Node.js apps with least privileges

2. High Severity Vulnerability (Python Tornado 6.5.0 DoS)

Vulnerability Covered:

- Plugin ID 237199

Simple Fix/Mitigation:

- Upgrade Tornado using: pip install --upgrade tornado

- Verify using: pip show tornado (Ensure version 6.5.0 or later)

General Mitigation:

- Implement input validation for all endpoints

- Use rate limiting to reduce risk of DoS attacks

3. Medium Severity Vulnerability (SSL Certificate Cannot Be Trusted)

Vulnerability Covered:

- Plugin ID 51192

Simple Fix/Mitigation:

- Obtain a valid SSL certificate from a reputable CA (e.g., Let's Encrypt, DigiCert, etc.)

- For development: use self-signed certs with caution

- Ensure complete certificate chain is installed

- Follow documentation for your server (e.g., Nginx, Apache, Node.js, Flask)

- Verify installation using tools like: https://www.ssllabs.com/ssltest/

General Mitigation:

- Automate renewal using Certbot (for Let's Encrypt)

- Monitor expiration dates with alerts