Critical Vulnerability Report

Vulnerability Name:

Node.js < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 Multiple Vulnerabilities

CVE IDs Involved:

CVE-2024-21892, CVE-2024-23019, CVE-2024-23018, CVE-2024-22017, CVE-2024-23016, CVE-2024-21894, CVE-2024-21889

Description:

The installed version of Node.js (v20.11.1) is outdated and vulnerable to multiple critical flaws. These include privilege escalation, memory leaks, path sanitization bypasses, cryptographic weaknesses, and configuration overwrites.

These issues may lead to arbitrary code execution, denial of service (DoS), unauthorized access, and sensitive data exposure.

Impact:

- Elevated system access
- Application/service compromise
- Crash or shutdown of critical services
- Exploitation by remote attackers

Affected Path:

/usr/lib/python3/dist-packages/playwright/driver/node

Tested Host:

192.168.1.47

Solution:

Upgrade Node.js to version 18.19.1 / 20.11.1 / 21.6.2 or later.

More Info: http://www.nessus.org/u?313add91

Mitigation Steps:

1. Identify applications using vulnerable Node.js versions.

2. Backup and remove outdated versions.

3. Install latest LTS version from https://nodejs.org.

4. Restart dependent services.

5. Re-scan to verify fix.