Nessus Vulnerability Scan Report

Tool Used: Nessus Essentials
Scan Type: Basic Network Scan
Target IP: 192.168.60.3
Scan Date: 2025-08-07

Vulnerability Summary:

Total Vulnerabilities Found: 83
Critical: 2
High: 3
Medium: 5+
Low/Informational: Multiple

Top Critical and High Vulnerabilities:

Severity	CVSS v3.0	Plugin ID	Plugin Name
Critical	9.8	190856	Node.js < 18.19.1 / 20.11.1 / 21.6.2
Critical	9.1	242134	Node.js < 20.19.4 / 22.17.1 / 24.4.1
High	8.2	192945	Node.js < 18.20.1 / 20.12.1 / 21.7.2
High	8.1	201969	Node.js < 18.20.4 / 20.15.1 / 22.4.1
High	7.7	214404	Node.js < 18.20.6 / 20.18.2 / 22.13.1

Remediation Recommendations:

• Update Node.js to the latest LTS version to fix known vulnerabilities.
• Upgrade supporting libraries such as SQLite, Ruby, and related components.
• Rotate and verify SSL/TLS certificates if flagged as expired or untrusted.
• Regularly patch and update all system dependencies and packages.

Conclusion:

The Nessus scan detected critical and high vulnerabilities on the target system. Immediate actions should be taken to apply security patches and update software to minimize the risk of exploitation. Regular vulnerability scanning is recommended to maintain security hygiene.