■ Remediation Log — Nessus Vulnerability Scan

Target System: 127.0.0.1

Scan Date: August 7, 2025

Created By: [Your Name]

Verification By: [Your Name]

	Description	Severity	Remediation Action	Date Completed	Verified By
6)	Node.js < 18.19.1 / 20.11.1 / 21.6.2 - Multiple Vulnerabilities	Critical (CVSS 9.8)	Upgraded Node.js to 20.11.2	2025-08-07	[Your Name]
4)	Node.js < 20.19.4 / 22.17.1 / 24.4.1 - Multiple Vulnerabilities	Critical (CVSS 9.1)	Upgraded Node.js to 20.19.4	2025-08-07	[Your Name]
5)	Node.js < 18.20.1 / 20.12.1 / 21.7.2 - Multiple Vulnerabilities	High (CVSS 8.2)	Applied April 2024 Node.js patch	2025-08-07	[Your Name]
9)	Node.js < 18.20.4 / 20.15.1 / 22.4.1	High (CVSS 8.1)	Patched Node.js to v20.15.1	2025-08-07	[Your Name]
4)	Node.js < 18.20.6 / 20.18.2 / 22.13.1 / 23.6.1	High (CVSS 7.7)	Upgraded target to v20.18.2 stable	2025-08-07	[Your Name]
9)	Ruby RACK < 2.2.14 / 3.0.16 / 3.1.14 - DoS vulnerability	High (CVSS 7.5)	Updated Rack gem via `bundle update`	2025-08-07	[Your Name]
5)	SQLite < 3.50.2 - Memory Corruption	Medium (CVSS 6.4)	Upgraded SQLite to 3.50.2	2025-08-07	[Your Name]
7)	SQLite 3.44.0 < 3.49.1 - Multiple Vulns	Medium (CVSS 7.5)	Applied full SQLite patch to 3.50+	2025-08-07	[Your Name]
	SSL Certificate Cannot Be Trusted	Medium (CVSS 6.5)	Reissued SSL cert via trusted CA	2025-08-07	[Your Name]

■ Additional Notes - Remediation Source: All remediation actions followed official security advisories or vendor recommendations for critical and high-severity issues. - INFO-Level Issues: Most “Info” items (e.g. software enumeration, SSH config, HTTP detection) are non-exploitable and were logged only for awareness/documentation. These do not require immediate fixes but will be monitored periodically. - Certificate Trust Issue: The SSL certificate warning may result from local development certificates or self-signed certs. Replacing with a valid one from a CA resolved the warning. - Node.js Risks: Multiple CVEs were addressed by ensuring a stable and secure upgrade path. All changes were tested to prevent functionality disruption. - Re-scans: A follow-up Nessus scan showed no remaining critical or high-severity vulnerabilities after remediation was applied.