Automated NPM Package Scanner

Post-Attack Remediation

QMASTERS

A Cross-Platform Guide for Vulnerability Detection and Reporting

Author: Mor Golan - QMasters

Date: November 27, 2025

Cross-Platform Detection and Workflow

Dual-Script Approach: Windows and Linux Scanning

Component	Windows Script	Linux Script	Purpose
Script File	find_impacted_packages.ps1 (PowerShell)	find_impacted_packages.sh (Bash)	Native execution on each OS type
Input File	impacted_packages.txt	(~800 vulnerable packages)	**Must be in the same directory**
Prerequisites	npm installed	npm + jq installed	If missing → Host is NOT infected
Scanning	npm list -g (global) & npm list (local)		Audits all installed packages

Workflow: Detection and Reporting

1. **Check Prerequisite:** Verify Node.js/NPM is installed.
2. **Scan:** Audit all installed packages against the impacted_packages.txt list.
3. **Report:** Display results on terminal AND send data to webhook.

Critical: If Node.js or NPM is not installed, the script exits immediately. Conclusion: Host is NOT infected by NPM packages.

Configuration and Reporting Options

Reporting Options: Terminal Visibility or Centralized Webhook

Output Channel	Visibility	Configuration	Content
Terminal Output	Immediate & Local	Default behavior	Color-coded summary with detected packages
Webhook Notification	Centralized & Instant	Edit WEBHOOK_URL variable	JSON payload with hostname, timestamp, packages

Configuration Example (Linux/Bash)

```
# Configuration section in find_impacted_packages.sh
WEBHOOK_URL="WebHook_HERE_FOR_DATA"# <-- EDIT THIS LINE
PACKAGE_LIST_PATH="./impacted_packages.txt"
OUTPUT_FORMAT="json"# Can be "json" or "csv"
```

Setup Requirements

Place both the script and impacted_packages.txt in the same directory

Ensure Node.js and NPM are installed on the target system

For Linux: Ensure jq is installed (JSON query tool)

Replace WEBHOOK_URL with your actual webhook endpoint

AWS Development: Ongoing work is focused on integrating this detection and reporting process with AWS services for enhanced scalability and centralized management across your infrastructure.