

**Redback Operations**

Vulnerability Management – Discovery, Analysis and Patching Recommendations (Critical Vulnerabilities)

18 September 2025



# Change / Run history

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version Details** | **Document Owner:** | **Prepared by:** | **Approved by:** | **Main Changes:** |
| **Revision: 01 18/09/2025** | **Ben Stephens** | John Hill | Ben Stephens | First Run. |

Table of Contents

[Change / Run history 1](#_Toc209119050)

[1. Introduction 3](#_Toc209119051)

[2. Tools utilized 3](#_Toc209119052)

[3. Discovery 4](#_Toc209119053)

[4. Vulnerability Analysis 5](#_Toc209119054)

[5. Vulnerabilities / Risk Assessment 6](#_Toc209119055)

[6. Recommendation 6](#_Toc209119056)

# Introduction

This document describes the architecture and framework utilized within Redback Operations to:

* Gather information around vulnerabilities determined by the Wazuh Toolset
* Prioritize vulnerabilities based on the ***Common Vulnerability Entry (CVE)*** and it’s related ***Common Vulnerability Score*** (based on the CVSS).
* Analyse such vulnerabilities for applicability to Redback Operations environment
* Advise (and provide recommendations) for treatment of vulnerabilities (translated into risk based on Likelihood \* Impact) deemed applicable to Redback Operations:
  + Avoid
  + Transfer
  + Accept
  + Mitigate

Such treatment may include application of a “patch” to mitigate the associated risk of the vulnerability, however a patch may not be available and it may be necessary of reduce the risk of compromise via discontinuation of the product with the vulnerability or upgrade of the product to a level (or release) not containing the vulnerability / risk.

# Tools utilized

Redback Operations executes the ***Wazuh*** product within it’s IT capability.

Wazuh is an open-source security platform which has the ability to collect data, perform vulnerability assessment and provide incident response (among other capabilities).

It does this by deployment of an endpoint security agent of an endpoint resource (in the Redback Operations VM instance, the agent is ***redback1.)***

The agent (after collecting data such as an inventory of software etc) sends the data to the server component (also, but not necessarily) running on the same O/S instance which performs the necessary function. Use of a web-based dashboard provides centralized management and visualization of the endpoint being monitored.

Figure 1 shows the architecture of Wazuh.

A screenshot of a computer

AI-generated content may be incorrect.

Figure Wazuh architecture

# Discovery

As per section 2, the deployed agent ***redback1*** collected inventory of “discovered” vulnerabilities By using the dashboard, Figure 2 shows the high level visualization. Our immediate interest lies within the ***Critical – Severity*** widget. It shown 17 vulnerabilities classified (by Wazuh through it’s CVSS repository).

A screenshot of a computer

AI-generated content may be incorrect.

Figure Wazuh Vulnerability Detection High Level Dashboard

Next step is to dig down deeper into the 17 vulnerabilities as these should be our immediate priority to analyse and treat (where applicable).

Figure 3 shows a deeper dive snapshot of the Critical vulnerabilities along with the agent name: redback1, the related package and version, a description of the vulnerability ***and*** the CVE vulnerability ID correlated through externally obtained (from MISP, Threatdata and Microsoft etc) threat intelligence data by Wazuh.

A screenshot of a computer

AI-generated content may be incorrect.

Figure Snapshot of critical vulnerabilities

The data was downloaded for the analysis step as shown in Table 1.



Table Data (CVE's) for analysis

# Vulnerability Analysis

As can be seen within the downloaded data, there are 8 unique CVE’s classified as critical severity. Each was analysed, with the resultant analysis shown in Table 2.



Table Analysis of critical CVE's

Overall, of the eight (8) unique critical vulnerabilities, 6 were found to be either not applicable to the current software inventory deployed within Redback Operations VM instance, one (CVE-2025-27558) was recent and still under investigation with one (CVE-2021-3773) having no patch available.

# Vulnerabilities / Risk Assessment

The potential impact / inherent risk of unpatched vulnerabilities to Redback Operations is shown in Table 3.



Table Vulnerability Assessment

# Recommendation

Recommendation for the 2 critical vulnerabilities is that both are assessed as low risk that both associated risks are accepted by Redback Operations.

These may be remediated (although effort is required) by a potential upgrade of Linux 5.15.0-153 to a later version of Linux image sans the vulnerability although I note two packages of Linux present. De-installation of the unused version should be undertaken as a general housecleaning exercise.