

**Redback Operations**

Vulnerability Management and Patching Standard

16 September 2025



# Change history

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version Details** | **Document Owner:** | **Prepared by:** | **Approved by:** | **Main Changes:** |
| **Revision: 01 16/09/2025** | **Ben Stephens** | John Hill | Ben Stephens | Original Issue. |

Table of Contents

[Change history 1](#_Toc208928435)

[1. What is this Standard about? 3](#_Toc208928436)

[2. Introduction 3](#_Toc208928437)

[2.1. To whom does this Standard apply? 3](#_Toc208928438)

[2.2. Standard review 3](#_Toc208928439)

[3. General principles 3](#_Toc208928440)

[4. Roles and responsibilities 4](#_Toc208928441)

[5. Software registers 4](#_Toc208928442)

[6. Scanning for vulnerabilities 4](#_Toc208928443)

[7. Assessing the criticality of vulnerabilities 5](#_Toc208928444)

[8. Remediating vulnerabilities 6](#_Toc208928445)

[9. Managing unsupported software 6](#_Toc208928446)

# What is this Standard about?

This Standard describes Redback Operations approach to vulnerability management.

Vulnerability management is the process by which the vulnerabilities identified through scanning are monitored, evaluated, prioritized and managed until the vulnerabilities are remediated. Vulnerability management ensures that appropriate actions are taken to reduce the potential that these vulnerabilities are exploited and thereby reduce risk of compromise to Redback Operations technology assets.

# Introduction

# To whom does this Standard apply?

This Standard applies to all technologies within Redback Operations.

# Standard review

This Standard will be reviewed every (three) 3 years unless circumstances necessitate more frequent updates.

# General principles

As per the Cyber Security Policy, all technologies must be scanned for vulnerabilities.

Each technology must be inventoried and have an individual or group assigned responsibility for maintenance and administration.

All technologies require a vulnerability management approach regardless of the location of that technology (e.g. cloud or on-premises) and connectivity external or internal networks.

Vulnerability management practices must follow a structured approach to ensure consistent and methodical identification, assessment and remediation of vulnerabilities.

Vulnerabilities are to be assessed for their potential business impact and risk.

Vulnerability management should be centralized to provide holistic visibility of security posture across Redback Operations.

Vulnerability management should follow relevant controls pertinent to Maturity Level 1 of the ASD Essential Eight Framework.

If patches are not available for vulnerabilities, compensating controls are to be identified to reduce the risk of compromise such as discontinuation of the product with the vulnerability or upgrade of the product to a level (or release) not containing the vulnerability / risk.

# Roles and responsibilities

|  |  |
| --- | --- |
| **Team** | **Responsibility** |
| **Cyber** | * Maintaining policies and standards vulnerability management. * Monitoring multiple sources of information on threats and vulnerabilities. * Facilitating vulnerability identification, prioritization, remediation deployment and remediation scanning. |
| **Asset Owners** | * Accepting and owning risk of non-conformance to cyber security requirements. |
| **Technology Operations** | * Incident management. |
| **Infrastructure Team** | * Undertaking patching, updates and upgrades of software. |
| **All Staff / Users** | * Complying with this Standard. * Reporting vulnerabilities to the Technology Operations or Cyber team. |

# Software registers

A software register for Redback Operations servers is required to be developed and maintained.

The software register is required to contain versions and patch histories of applications, drivers, operating systems and firmware.

# Scanning for vulnerabilities

An automated method for asset discovery is required to be used to detect assets for subsequent vulnerability scanning activities.

Vulnerability scanning must address missing patches and updates for vulnerabilities.

Online services are required to be scanned **daily**.

Web browsers and their extensions should be scanned **weekly** for vulnerabilities.

Drivers and firmware to be scanned **every month**.

# Assessing the criticality of vulnerabilities

The potential impact of vulnerabilities to Redback Operations is required to consider vendor ratings, industry ratings such as the Common Vulnerability Scoring System (CVSS) score, controls that have been implemented to reduce the risk of compromise, and the potential business impact if a vulnerability is exploited within the control environment.

Automated tools should be used where possible to quickly and consistently calculate the potential impact and reachability of a vulnerability and assign a priority for remediation.

The risk of a vulnerability being exploited must consider multiple environmental factors including:

* Internet reachability. Vulnerabilities that are exploitable via internet facing systems pose a higher risk. Note that a vulnerability in a non-internet-facing component could still be critical if exploited through chained attacks.
* Functional reachability. This determines whether a vulnerability is exploitable within the context of an application. For example, if functions associated with vulnerabilities are actively called in the application.
* Dependency-level reachability. Dependency-level reachability examines whether a vulnerable package is imported or called anywhere in the application. This provides a basic layer of prioritization by identifying unused dependencies that can be safely removed.
* Package baselining. Assesses the behavior of third-party libraries to identify unusual or malicious actions. For example, a logging library like Log4j should not execute code or make network calls under normal circumstances. If it does, this would likely indicate an active exploit.
* Controls in place to reduce the risk of compromise. Controls within the environment may make reaching a vulnerability more difficult or not possible which can downgrade the urgency for remediation.

The following table should be used to guide the criticality and prioritization of vulnerabilities.

|  |  |  |
| --- | --- | --- |
| **CVSS** | **Severity** | **Maximum Remediation Timeframe** |
| 9.0 to 10.0 | **Critical** | **7 days** |
| 7.0 to 8.9 | **High** | **14 days** |
| 4.0 to 6.9 | **Medium** | **30 days** |
| 0.1 to 3.9 | **Low** | **45 days** |

# Remediating vulnerabilities

Patching activities are required to address applications; operating systems of servers, network devices and IT equipment; and firmware and drivers.

Vulnerabilities in online facing applications and, operating systems of internet-facing servers and network devices are to be prioritized for remediation.

Patching of Critical risk vulnerabilities should commence within 48hours of release and should be completed within a maximum of 7 days.

High risk vulnerabilities should be analysed and patched or remediated within 14 days.

Medium risk vulnerabilities should analysed and patched or remediated within 30 days.

Low risk vulnerabilities should be analysed and patched or remediated within 60 days.

If patches are not available, alternate risk mitigation controls are required to be implemented including changing system configuration settings; disabling ports, protocols and services; removing impacted software and/or functions; strengthening security controls around the impacted technology; and upgrading the component to treat the vulnerability.

The successful remediation of vulnerabilities is required to be confirmed by rescanning vulnerable technologies and checking the implementation of patches or changes to configuration.

# Managing unsupported software

Any software including online services, applications, extensions, security products, operating systems, network devices and networked-IT equipment should be removed or replaced / upgraded before reaching end of support.

If unsupported software cannot be immediately removed or replaced, alternate controls must be documented and implemented to reduce the risk of compromise, and an exemption must be sought from the Cyber team.