Sharing allow:
TLP - GREEN

Approved

Vulnerability Management Standard

Document ID: **SEC-04**
For: Alliance Federation
Approval Date: 2022-08-24
Approved By: NSC

1. Introduction

A compromise due to software or configuration vulnerabilities threaten the confidentiality, integrity and availability of the Digital Research Alliance of Canada Federation ecosystem and connected devices. Vulnerability management is a security measure intended to prevent the exploitation of Information Technology (IT) vulnerabilities that exist within the Alliance Federation. By taking a proactive approach to managing software with known vulnerabilities, the Alliance Federation can reduce or eliminate the potential for exploitation.

The purpose of this standard is to define the requirements for the remediation of vulnerabilities within the organization. To accomplish this, the standard describes the roles involved, the treatment of vulnerable systems, levels of vulnerability severity, and the timeframes in which vulnerabilities under these levels must be addressed.

2. Definitions

Refer to *SEC-00 Information Security Glossary* definitions used in this Standard

- **Vulnerability**: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
- **Severity**: the degree to which a vulnerability could impact Alliance Federation systems or data.

3. Applicability

3.1. This standard applies to infrastructure that supports Alliance Federation Systems and Services.

4. Vulnerability Management

These sections provide guidance and instruction for each step in the vulnerability management lifecycle.

4.1. Lifecycle roles and responsibilities (RACI matrix)

	CSAC and/or OSAC	**TLC**	**NSC**	**Security Operations**	**Risk Owner**	**Service Owner**	**Alliance Comms**
Maintain general vulnerability awareness and security posture (4.2.1)			A	R		I/R	
Vulnerability detection (4.2.2)			A	R			
Assessing the severity and required timings to address a vulnerability = Severe (4.2.3)	I	I	A	C	R	C	C
Assessing the severity and required timings to address a vulnerability = High (4.2.3)		I	A	C	R	C	C
Assessing the severity and required timings to address a vulnerability = Medium (4.2.3)			A	C	R	C	C
Assessing the severity and required timings to address a vulnerability = Low (4.2.3)			A	C	C	R	C
Treating the vulnerable system or service (4.2.4)			I	C	A	R	
Measurement and Reporting (4.2.5)	I		A	R		C	

Table 1: RACI Matrix - Responsible, Accountable, Consulted, Informed

4.2. Lifecycle

4.2.1 Maintain general vulnerability awareness and security posture

4.2.1.1 Security Operations should keep abreast of mailing lists, social media, and other cybersecurity news sources for vulnerability information.

4.2.1.2 Service Owners should avail themselves of various information sources with respect to their systems and services to know when vulnerabilities have been announced.

4.2.1.3 Unused services on servers should be disabled, and operating systems and applications should be hardened against external threats.

4.2.1.4 Service Owners must ensure that Alliance Federation assets use versions of software that are actively patched and hardened against vulnerabilities. End of Life (EOL) software should not be used.

4.2.2 Vulnerability detection

- Security Operations staff are authorized and responsible for vulnerability scanning under the terms of this standard.
- Automated scanning of all Alliance Federation assets will be performed at a minimum of once per month, or manually on a per-case basis when working to identify and address Severe vulnerabilities.
- All vulnerabilities labeled *Medium* or higher in *Table 2: Assessment and Handling* below will be handled as per the vulnerability response procedure.

4.2.3 Assessing the severity and required timings to address a vulnerability

- Common Vulnerability Scoring System (CVSS) scores are assessed by MITRE and available at the US National Vulnerability Database (NVD). Obtain the CVSS base score for each vulnerability, and taking into account local protective measures and mitigations, consult the *Treatment target* column in *Table 2: Assessment and Handling* below for target treatment times.

Category	**Score**	**Treatment target**	**Exception Parties**	**Exception target**
	CVSS base score[1]	*Target timeframe for initial mitigation and treatment once available*	*Responsible Party able to grant exceptions to treatment targets*	*Maximum timeframe within which exceptions must be reviewed and re-granted*
Severe	9.0-10.0	<1 business day	Risk Owner (required to inform OSAC and TLC)	6 months
High	7.0-8.9	<10 business days	Risk Owner (required to	12 months

[1] Based on the latest CVSS version, which is at the time of writing v3.1.

			inform TLC)	
Medium	4.0-6.9	<20 business days	Risk Owner	18 months
Low	0.1-3.9	discretionary	Service Owner	24 months

Table 2: Assessment and Handling

- Exceptions to the timeframes in the *Treatment targets* column must be handled according the the following process depicted and described in *Figure 1: Target Timeframe for Mitigation*:

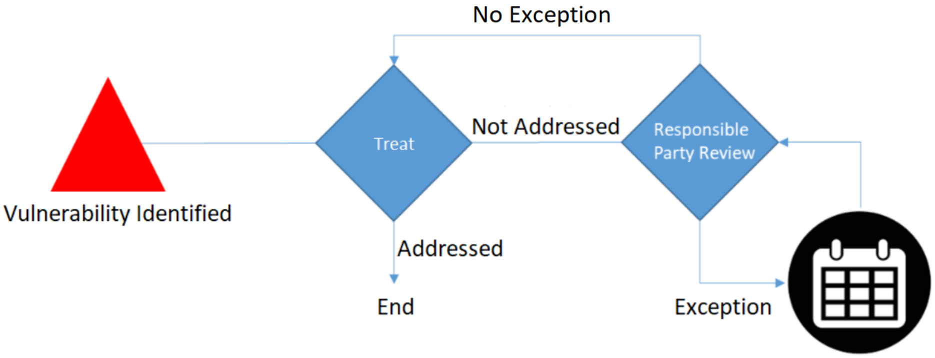

Figure 1: Target Timeframe for Mitigation

- Those indicated in the *Exception Parties* column must review and record in the Alliance Federation risk register which vulnerabilities can remain untreated beyond the time indicated in the *Treatment target* column, and must also re-grant all exceptions within the time period indicated in the *Exception targets* column.
- Assets that are fragile to the scanning process must be added to the risk register and will be exempted from scanning if the Risk Owner accepts the risk.
- In cases where a vulnerability is suspected and a CVSS score is not available, Service Owners or delegates must submit details on the vulnerability to the NSC for review and analysis, and agreement among >=2 NSC members will be required to trigger the response process.
- In cases where a vulnerability is likely to impact a significant number of cloud-based virtual machines, a communication should be sent to cloud project owners notifying them of the vulnerability and how to mitigate the risk. Alliance Federation's Communications team will be consulted.
- For *Severe* vulnerabilities, OSAC and CSAC must be notified, in consultation with Alliance Federation's Communications team.

4.2.4 Treating the vulnerable system or service

- The Vulnerability Response procedure must be followed for all vulnerabilities *Medium* or higher as per *Table 2: Assessment and Handing*.
- Upon successful treatment of *High* or *Severe* vulnerabilities, the Service Owner must notify the Security Operations team so that the asset can be re-scanned. Alternatively, the next regular scan will validate the success of the treatment.
- If a responsible party suspects that a vulnerability finding may be a false positive, upon confirmation with Security Operations staff, appropriate due diligence will be taken to address the false positive.
- As vulnerabilities can result in insights into risks and/or opportunities for new controls, Service Owners should use such occurrences to consider how their systems are hardened and what controls could be used to protect against similar vulnerabilities.

4.2.5 Measurement and Reporting

- Metrics, KPI, and Reports will be tracked and created by the Security Operations National Team, for reporting to the NSC.

5. Related Information

SEC-00 Information Security Glossary
Vulnerability Management Procedure
Change, Deployment and Hardening Systems Standard