NAM-CSIRT Vulnerability Coordination and Disclosure Policy

Issued by: Namibia Cyber Security Incident Response Team (NAM-CSIRT)

Effective date: 12 September 2025

Contents

1. NAM-CSIRT Identity & Mandate

1.1 The NAM-CSIRT is responsible to contribute to security and stability of critical infrastructure and critical information infrastructure of the Republic of Namibia.

1.2 Contact:

1.2.1 Phone: +264 61 222 666

1.2.2 Email: info@nam-csirt.na

2. CVE Numbering Authority (CNA)

2.1 The purpose of the policy is for the Common Vulnerability Exposure (CVE) Program CVE Numbering Authority (CNA) and to define NAM-CSIRT's authority, scope, and practices for coordinating disclosure of vulnerabilities.

2.2 NAM-CSIRT will act as a CVE Numbering Authority (CNA) for vulnerabilities meeting the following criteria:

2.2.1 Reported to NAM-CSIRT by researchers, users or organisations

2.2.2 Not already in scope of another CNA. If another CAN is responsible for the affected product, NAM-CSIRT will refer to the report.

3. Coordination & Disclosure Process

3.1 Submission

3.1.1 Vulnerability reports should include:

3.1.2 Product name & version

3.1.3 Clear detailed description of the vulnerability

3.1.4 Impact of vulnerability (confidentiality, integrity, availability)

3.1.5 Steps to reproduce or PoC,

3.1.6 Any deadlines or prior commitments by reporter.

3.2 Acknowledgment

3.2.1 NAM-CSIRT will acknowledge receipt within 5 business days.

3.3 Notification & Coordination

3.3.1 NAM-CSIRT will contact the responsible party to facilitate remediation. NAM-CSIRT may assist reporter with vendor contact if needed.

3.4 Public Disclosure

3.4.1 Once a patch or mitigation is available, or after a reasonable deadline (generally 120 days from initial contact), NAM-CSIRT may publish an advisory.

3.5 CVE Assignment

3.5.1 For vulnerabilities under NAM-CSIRT's scope, NAM-CSIRT will assign a CVE ID and publish details consistent with CVE Program rules.

4. Exclusions & Limitations

4.1 NAM-CSIRT will not accept or act as CNA for reports that:

4.1.1 Already handled or owned by another CNA

4.1.2 Outside NAM-CSIRT's mandate

4.1.3 Products no longer maintained or that pose negligible risk

4.1.4 Duplicate report of publicly known vulnerabilities

5. Public Advisories & Transparency

5.1 NAM-CSIRT publishes advisories on its official website (nam-csirt.na) under its "Alerts / Security Advisories" or "Resources" pages.

5.2 Advisories will include description of the vulnerability, affected products/versions, impact assessment, mitigation or remediation steps, and a CVE identifier (if assigned).

5.3 Exploit code will not be published (unless low-risk, or only as proof of concept carefully controlled).

6. Disclaimer

6.1 Whilst every precaution will be taken in preparation of information, notification and alerts, NAM-CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information it provides. alerts, NAM-CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information it provides.

Namibia Cyber Security Incident Response Team (NAM-CSIRT)

Hosted @Communication Regulatory Authority of Namibia

Tel: +264 61 222 666 Email: info@nam-csirt na

_____ END _____