Nozomi Networks Labs Vulnerability Disclosure Policy

The goals of the Nozomi Networks, Inc. Labs ("Nozomi Networks Labs") Vulnerability Disclosure Policy are two-fold:

1. Protect end users in a timely manner, by ensuring that the vendor is acting promptly on the information provided to resolve the issue; and
2. Ensure that the action is as comprehensive as possible, such that it will fix the vulnerability thoroughly without causing further risks to the end users.

To achieve these goals, Nozomi Networks Labs adopts the following disclosure timeline.

Phase 1: Vendor Notification

Deadline: Day 30

Nozomi Networks Labs will attempt to contact the vendor, either directly or indirectly via a **CVE Numbering Authority of Last Resort** (CNA-LR).

Nozomi Networks Labs will provide the vendor with a vulnerability advisory report containing an overall description of the issue, an in-depth technical analysis, possible remediation suggestions, and a copy of this vulnerability disclosure policy.

The vendor has up to 30 days to reply from the initial disclosure, acknowledging that the issue is under analysis.

Nozomi Networks Labs will attempt to notify the vendor via the established communication channel if they fail to meet this deadline.

Phase 2: Vendor Engagement

Deadline: Day 60

The vendor has to reply within 60 days maximum from the initial disclosure, producing:

1. A technical explanation of how the issue will be addressed; and
2. A timeline for the public disclosure.

Nozomi Networks Labs will attempt to notify the vendor via the established communication channel if they fail to meet this deadline.

Nozomi Networks Labs will review the provided information and, if necessary, start a discussion with the vendor with the aim of reaching a mutually-agreed action.

Phase 3: Public Disclosure

Deadline: Day 120

The vendor has to publicly resolve the vulnerability in 120 days maximum from the initial disclosure.

After the vendor has publicly resolved the issue, or after 120 days from the initial disclosure (whichever comes first), Nozomi Networks Labs will release a public notification of the vulnerability and, at our discretion, a technical blogpost of the issue.

Timeline Extensions

Nozomi Networks Labs is aware that some vulnerabilities can have profound ramifications on the affected systems. For this reason and on a case-by-case basis, Nozomi Networks Labs is open to discussing a timeline extension, provided, however, that the vendor satisfactorily illustrates to Nozomi Networks Labs the technical rationale behind the request.

At any stage of this process, Nozomi Networks Labs is fully committed to working with vendors to ensure that the technical details and severity of a reported security issue are fully understood. This is accomplished by sharing with the vendor technical information gathered through the research and—when possible—a reliable way to reproduce the issue.

If a vendor chooses not to take the actions requested herein and fails to meet the disclosure timeline, or is unable to provide a sound explanation for not meeting the expectations, Nozomi Networks Labs, after 120 days from the initial disclosure, will publish an advisory with limited technical details including mitigations.

In all the cases, Nozomi Networks Labs will formally and publicly release its security advisories.