VULNERABILITY DISCLOSURE POLICY

NetRise

Vulnerability Disclosure Policy Goals and Purpose

The primary goal behind disclosure of a vulnerability is quite simple. If NetRise can identify a vulnerability through automated and/or manual analysis of XIoT devices, firmware, or other binary files, it is likely that nefarious threat actors can identify the same vulnerability through a combination of automated and manual analysis. Therefore, the disclosure of the vulnerability (through proper channels) is much more likely to lead to a net-positive for the security community, and the ability for the affected vendor to supply a patch or mitigation strategy to its customers.

Scope Statement

Vulnerabilities in third-party Extended Internet of Things (XIoT) devices and firmware NetRise researches and analyzes which are not covered by another CNA.

Disclosure Process

NetRise's vulnerability disclosure process consists of two primary steps, the first of which is contacting the vendor to alert them of the finding and provide all relevant technical details, the second being public publishing of the vulnerability.

Vendor Contact

Upon identifying a non-published vulnerability, NetRise will attempt to make initial contact with the affected vendor through the following means:

- Leveraging official channels such as the vendor's PSIRT, whether this is through a web-form submission, email, or other channel
- If no such channel(s) exist, attempts will be made to reach out via other means such as a standard support form or email

Regarding disclosure timelines, NetRise will adhere to the following:

1. An initial contact will be made (leveraging the channels listed above) as soon as NetRise has collected all relevant information regarding the vulnerability
2. If no response is received from the vendor, NetRise will make a second attempt between 7-14 business days from the first contact
3. Similar to step two, if there is still no response received, NetRise will make a third attempt to contact the vendor between 21-30 business days from the first contact

If NetRise does not receive an adequate response from the vendor within 45 days of the initial contact attempt, NetRise will commence with the public disclosure process as applicable.

Vendor Disclosure Details

When disclosing a vulnerability to a vendor, NetRise will provide all available relevant information, which may include all of the following (and more, as applicable):

- Affected product(s) and components
- Details on the method of identification
- Whether or not the vulnerability has been manually verified
- Details regarding the timeframe for public disclosure of the vulnerability

    - Under most circumstances, vulnerabilities are published 90 days after initial disclosure to the vendor
- A ticket number for tracking purposes
- A link to this policy for reference

Vendor Response

Upon receiving a response from a vendor regarding a vulnerability, NetRise intends to work directly with them during the rest of the disclosure and remediation process and would appreciate this sentiment being reciprocated. This may include regular communication from the vendor regarding the following:

- Confirmation of the vulnerability from the vendor
- Status of the vulnerability confirmation and analysis
- Timetables regarding a patch or mitigation strategy being implemented by the vendor
- Any other relevant information regarding the internal analysis and mitigation of the vulnerability

NetRise is willing and prefers to work with vendors regarding the publication related to the vulnerability, which may include collaboration regarding messaging and strategy regarding the vulnerability at hand.

Public Disclosure

NetRise publishes identified vulnerabilities as Security Advisories to our website at www.netrise.io/security/advisories. As applicable, NetRise will include the following details in a disclosure:

- Technical details surrounding the identified vulnerability
- Proof-of-concept code if available
- Potential mitigation strategies, if applicable

Timetable

Given timely response from the vendor regarding an identified vulnerability, NetRise will provide all details regarding the timeframe for public disclosure, which is typically 90 days from the initial contact with the vendor. Vendors may request amendments to this timetable given extraneous circumstances, and such requests will be handled on an ad hoc basis.

Contacts

NetRise's vulnerability research team can be contacted at research@netrise.io