4RF Vulnerability Disclosure Policy

Introduction

4RF is committed to ensuring the safety and security of our customers and their field area network assets. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.
This document sets out the 4RF policy for accepting product vulnerability reports. We hope to foster an open partnership with the security community, and we recognize that the work the community does is important in continuing to ensure safety and security for all of our customers. We have developed this policy to both reflect our corporate values and to uphold our legal responsibility to good-faith security researchers that are providing us with their expertise.

This policy describes what systems and types of research are covered under this policy, how to send us vulnerability reports, and how long we ask security researchers to wait before publicly disclosing vulnerabilities.

We encourage you to contact us to report potential vulnerabilities in our systems.

Scope

The Vulnerability Disclosure Program covers the following products:

- Aprisa XE, Aprisa LE, and Aprisa XS
- Aprisa SR
- Aprisa SR+ and Aprisa FE
- Aprisa SRi
- Aprisa LTE

Researchers who submit a vulnerability report to us will be given full credit on our website once the submission has been accepted and validated by our product security team.

Legal Protection

4RF will not engage in legal action against individuals who submit vulnerability reports through our Vulnerability Reporting email address security@4rf.com. We agree not to pursue legal action against individuals who:

- Engage in testing or research without harming 4RF or our customers
- Engage in vulnerability testing within the scope of this vulnerability disclosure program
- Test products without affecting customers, or receive permission/consent from customers before engaging in vulnerability testing against their devices or networks
- Adhere to the laws applicable to their location and the location of 4RF
- Refrain from disclosing vulnerability details to the public before a mutually agreed-upon timeframe expires

How to Submit a Vulnerability

To submit a vulnerability report to the 4RF Product Security Team, please email us at security@4rf.com.

Guidelines

Under this policy, “testing” and “research” means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data
- Only use exploits to the extent necessary to confirm a vulnerability’s presence.
- Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or use the exploit to pivot to other systems
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly
- Do not submit a high volume of low-quality reports

Once you have established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must stop your test or research, notify us immediately, and not disclose this data to anyone else**.

The following test or research activities are not protected and are specifically not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Physical testing (e.g. over-the-air transmission without appropriate regulatory permission or license) or social engineering non-technical vulnerability testing

Preference, Prioritization, and Acceptance Criteria

We will use the following criteria to prioritize and triage submissions. What we would like to see from you:

- Well-written reports in English will have a higher chance of resolution
- Reports that include proof-of-concept code or other means to equip us to re-create the problem to better triage
- Reports that include only crash dumps or other automated tool output may receive lower priority
- Please include how you found the bug, the impact, and any potential remediation
- Please include any plans or intentions for public disclosure

What you can expect from us:

- A timely response to your email (within 5 business days)
- After triage, we will send an expected timeline, and commit to being as transparent as possible about the remediation timeline as well as on issues or challenges that may extend it
- An open dialog to discuss issues
- Notification when the vulnerability analysis has completed each stage of our review
- Credit after the vulnerability has been validated and fixed

If we are unable to resolve communication issues or other problems, 4RF may bring in a neutral third party (such as CERT/CC ,ICS-CERT, or the relevant regulator) to assist in determining how best to handle the vulnerability.

Questions

Questions regarding this policy may be sent to **security@4rf.com**. We also invite you to contact us with suggestions for improving this policy.

This document Version 1.1 was created 16 October 2020 based on advice from the US National Telecommunications and Information Agency (NTIA) Safety Working Group. Any updates will be noted below in the version notes.

Document change history

Version	Date	Description
1.1	16 October 2020	First issue