Cybersecurity Vulnerability Management Policy

Moxa has robust procedures in place to ensure that we can respond to any potential product[i] cybersecurity vulnerabilities. We continuously strive to provide reliable guidance and solutions so our clients can minimize risks. Therefore, Moxa has established the Product Security Incident Response Team (PSIRT), which is responsible for addressing product cybersecurity incidents and potential flaws in Moxa's products. In a relentless push to apply practices and standards[ii] adopted and recognized by the automation industry globally, Moxa ensures that the best process and response measures are used to address potential cybersecurity vulnerabilities. Moxa embraces industrial Internet security and remains a very reliable partner to all our clients.

Product Cybersecurity Vulnerability Management Process

Moxa's product cybersecurity vulnerability management process encompasses the five stages detailed below. Each stage involves processes and practices that Moxa carefully follows.

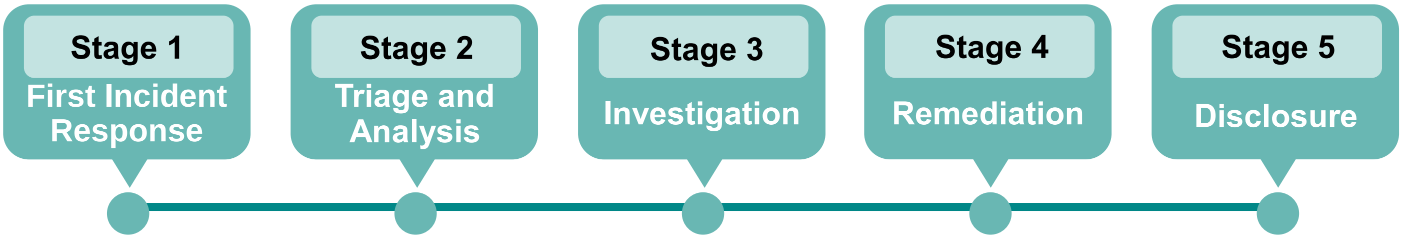

Figure 1. Management process for cybersecurity vulnerabilities

- **First Incident Response**: As soon as PSIRT receives an external vulnerability report regarding a Moxa product, we will send an initial response within two working days.
- **Triage and Analysis**: PSIRT triages and analyzes the possible cybersecurity vulnerability and assesses its impact on Moxa products. We will provide a preliminary assessment report at the end of this stage to the person who reported the vulnerability.
- **Investigation**: PSIRT works closely with the product development team to identify the root cause of the vulnerability and the degree, as well as the extent, of its impact on Moxa products. Next, PSIRT offers solutions to mitigate and solve the issue. During this stage, PSIRT continues to communicate with the person who reported the incident.
- **Remediation**: PSIRT works closely with the product development team to develop the final software/firmware patches or to finalize the mitigation measures. Meanwhile, PSIRT continues to follow any updates regarding relevant vulnerabilities to assess their potential impact. If the vulnerability poses a high risk for customers, and the development of the

final patch takes longer than the customer can wait, Moxa will provide temporary mitigation measures before the final patch becomes available.

- **Disclosure**: PSIRT will publish the results of the product cybersecurity vulnerability on the Security Advisory section of our website. The report will include a description of any vulnerabilities, the products and versions that are affected, mitigation measures, and remediation plans where appropriate.

Moxa's PSIRT and development team leverages the Common Vulnerability Scoring System (CVSS) and Moxa's Risk-based Vulnerability Management Model to assess the potential risks of an incident. PSIRT will create a timeline to address the issue based on several factors: the security context, the possibility of vulnerabilities being exploited, possible impacts, and other factors.

After analyzing the reported vulnerability, Moxa will immediately set up a designated testing environment to determine the severity of the vulnerability. When appropriate, Moxa will continue to communicate with the person who reported the issue. After identifying the root cause and possible severity of the impact, Moxa will proceed to remediation analysis and offer solutions or mitigation measures.

Our security advisory updates and announcements can be found on the Security Advisories section of Moxa's website and anyone can subscribe to the Security Advisories RSS Feed. If you would like to receive the latest security announcements for specific Moxa products, you have to create an account on Moxa's website first, before clicking the 'Follow Updates' option.

How to Contact Us About Cybersecurity Vulnerabilities

If you find a potential vulnerability in any of Moxa's products, please report it to us immediately. For Moxa, timely identification of any vulnerabilities is key to minimize security risks to our products. You can report any potential cybersecurity vulnerabilities on Moxa products by emailing PSIRT and use Moxa's PSIRT PGP key to encrypt files.

When reporting cybersecurity vulnerabilities, please include the following information to help us speed up performing a risk assessment and the subsequent development of remediation or mitigation measures:

1. Product name and model
2. Firmware/Software version

3. Equipment and software needed to reproduce issues
4. Steps to reproduce issues (attach pictures or codes if available)
5. Proof-of-concept exploit code
6. Description of how attackers can take advantage of the vulnerabilities
7. Capture the packets (use a tool, such as Wireshark, to achieve this)
8. Anything else that you feel may be relevant

- PSIRT email address: PSIRT@moxa.com
- Download Moxa's PGP key

Disclaimer

Content of the 'Cybersecurity Vulnerability Management Policy' may change depending on the circumstances of specific cases. We do not guarantee to respond to specific issues or categories of issues. You will be responsible for the risks taken when using any information in this document or any content linked through this document. Moxa reserves the right to change any content in this document at any time without prior notice. Any changes to the document will be published on Moxa's official website: www.moxa.com.

[i] The 'Product' as mentioned in this document refers to any standard Moxa product in the market. Maintenance and responses to flaws of non-standard products, such as customized products, will be carried out as stipulated in the contract.

[ii] Moxa follows a number of standards, including:

- Common Vulnerability Scoring System by FIRST (Forum Incident Response and Security Teams)
- PSIRT Services Framework v1.1 by FIRST
- ISO/IEC 29147:2018 Vulnerability Disclosure