



Vulnerability Disclosure Program

Thank you for working with Qmulos to help us address security issues with our products in a timely manner. Qmulos supports responsible disclosure of security vulnerabilities. We are committed to working with researchers in a professional and positive manner to protect our company and our customers. We encourage anyone who believes he/she has identified a vulnerability in our products to notify us by sending an email to vuln_disclosure@qmulos.com.

To help ensure that we have enough information to properly evaluate a potential issue, Qmulos requests that you include the following information in your email:

- Clear description of the issue explaining the vulnerability
- Evidence of the vulnerability such as logs, screenshots, responses, etc.
- Tools used in discovering the vulnerability
- Detailed steps to reproduce the issue
- An assessment of the exploitability or impact of the issue
- Affected product and version, e.g., Q-Compliance V4.0.0
- Other relevant software names and versions (Splunk, operating system, browser, etc.) • Date of discovery
- Name and contact details
- Any vulnerability database identifier you have requested. If you have not requested a CVE identifier, indicate if you would like us to request one.

Once we receive your report, Qmulos will stay in touch with you to provide updates on our investigation and status of a fix for verified issues. We may also request additional information from you during this time. If the issue you reported is determined to be valid and affects one of our products, an advisory will be published when a solution is available for our customers.

Qmulos does not participate in a public bug bounty program or provide financial awards for finding issues. In addition, Qmulos will not respond to:

- Hoaxes or anonymous reports
- Reports that are generic or lack evidence to be verified
- Reports that bear no relevance to Qmulos as a company, our products, our employees, or our customers
- Reports that are non-actionable

While we encourage you to discover and report to us any vulnerabilities you find in a responsible manner, the following activities are prohibited:

- Performing actions that may negatively affect Qmulos or our customers
- Accessing, or attempting to access, data or information that does not belong to you
- Destroying or corrupting, or attempting to destroy or corrupt, data or information that does not belong to you
- Conducting any kind of physical or electronic attack against Qmulos personnel or property
- Social engineering any Qmulos employee or contractor
- Violating any laws or breaching any agreements in order to discover vulnerabilities

Thank you for helping to keep Qmulos secure!

We appreciate the efforts of the security research community who work to identify vulnerabilities and collaborate with organizations like ours to create a fix and communicate responsibly to affected parties.