Responsible Vulnerability Disclosure Policy

We take the security of our systems seriously and we welcome feedback from security researchers in order to improve the security of our products and services.

We require that all researchers take into account the respect for the law. Vulnerability scanning could not serve as a pretext for attacking a system or any other target. Several actions must be avoided. For example:

- Using social engineering
- Compromising the system and persistently maintaining access to it
- Changing the data accessed by exploiting the vulnerability
- Using malware
- Using the vulnerability in any way beyond proving its existence. To demonstrate that the vulnerability exists, the reporter could use non-intrusive methods. For example, listing a system directory
- Using brute force to gain access to systems
- Sharing vulnerability with third parties
- Performing DoS or DDoS attacks

Keep information about any vulnerabilities you’ ve discovered confidential between yourself and Salto Systems until we resolve the issue.

Send an email to securityalert@saltosystems.com if you have identified any issue that potentially can affect the security of our products or services.

We will promptly acknowledge receiving your report.