Qlik® Security Vulnerability Policy

September, 2015

Reporting

Qlik takes the security of our products seriously. We have a dedicated team of security experts working on testing, hardening and securing our products. We also work closely with external security companies, our customers and partners to ensure the security of our products is of the highest standard. If you discover a suspected security vulnerability, please report it to our support team immediately.

Investigation

When our support team receives a vulnerability report, they will immediately inform our security team who will contact the reporter to attain details of the vulnerability in a secure way. Our security team will work together with the reporter to understand the potential impact of the issue and its likelihood of being exploited. Based on this information, our security team will make an independent assessment of the security classification of the vulnerability.

Credit

Qlik® appreciates the efforts that external parties make in helping us to secure our software. We ask that anyone finding a security vulnerability report the issue to us first, then collaborate with us to allow our security team a reasonable amount of time to investigate the issue and create a fix, before going public with the security vulnerability.

Qlik® will credit the finders of security vulnerabilities in the release notes for the fix.

Disclosure

In instances where a reported vulnerability is classed as high or critical by our security team, and the vulnerability has *not* been exploited in the wild, Qlik will follow the disclosure policy known as ***Responsible Disclosure***.

Qlik® will:

- Create a software fix that addresses the vulnerability and make it available to our customers and partners.
- Collaborate with the reporter of the vulnerability to schedule an external disclosure, announcing when a fix will be available.
- Publish a Security Bulletin in our customer and partner portals that details the security vulnerability and states when a fix will be available.

In instances where a reported vulnerability is classed as high or critical by our security team, and the vulnerability has been exploited in the wild,

Qlik® will:

- Publish a Security Bulletin with details of the security vulnerability, including possible mitigation actions. The Security Bulletin will be published as soon as possible after the vulnerability has been reported and assessed.
- Collaborate with the reporter of the vulnerability for its external disclosure.
- Create a software fix that addresses the vulnerability and make it available to our customers and partners as soon as possible.

In instances where a reported vulnerability is classed as low or medium, Qlik may publish a Security Bulletin with details of the reported vulnerability in our customer and partner portals, and a fix for the issue will be delivered in the next Service Release after its remediation.