Vulnerability disclosure policy

BT Redcare are a leading provider of alarm signalling devices and services which enable fire, security and more to be monitored over a secure network - keeping homes and businesses safe.

We take safety and security very seriously and appreciate those who take the time and effort to report a vulnerability according to our policy. However, we do not offer monetary rewards for vulnerability disclosures.

This vulnerability disclosure policy covers BT Redcare’s Next Generation portfolio.

We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always acting in compliance with it.

If you believe you have found a security vulnerability, please submit your report to us at redcarefaults@bt.com.

To helps us we ask you to include the following in your report:

\* The product where the vulnerability can be observed

\* A detailed description of the vulnerability

\* Steps to reproduce. These should be a benign, non-destructive, proof of concept

This will help to ensure that the report can be acted upon quickly and accurately. It also reduces the likelihood of duplicate reports. We may ask you to provide additional information if necessary.

**What to expect from us**

After you have submitted your report, we will initially respond with an automated email, we will then confirm within 5 working days and aim to triage your report within 20 working days. We’ll also aim to keep you informed of our progress.

As you will be aware vulnerability reports can take some time to triage or address. You are welcome to enquire on the status but should avoid doing so more than once every 15 working days. This allows our teams to focus on resolving the issue.

We will notify you when the reported vulnerability is fixed, and you may be invited to confirm that the solution covers the vulnerability adequately.

Once your vulnerability has been resolved, we welcome requests to disclose your report. We’d like to manage the guidance to affected users, so please do continue to coordinate public release with us.

Vulnerability software fixes are estimated to be made available to users no later than 90 days following acknowledgement of receipt.

**Policy guidance**

We would expect you to NOT:

* Break any applicable law or regulations
* Access unnecessary, excessive or significant amounts of data
* Modify data in our systems or services
* Use high-intensity invasive or destructive scanning tools to find vulnerabilities
* Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests
* Disrupt our services or systems
* Communicate any vulnerabilities or associated details
* Social engineer, ‘phish’ or physically attack our staff or infrastructure
* Demand financial compensation in order to disclose any vulnerabilities

We would expect you to:

* Always comply with data protection rules and must not violate the privacy of our users, staff, contractors, services or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
* Keep information about the potential vulnerability in confidence between yourself and us until we have a fix in place
* Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause BT Redcare to be in breach of any legal obligations.