RFC2350 Description for: British Telecommunications CERT Co-ordination Centre (BTCERTCC)

1. About this document

We provide basic information about our team. We include our contact information, what we are responsible for and services we may be able to offer. We do this to comply with RFC2350.

We use the terms "we" and "us" to mean BTCERTCC. We use the term "our" to mean belonging to BTCERTCC.

We use the term “BT” to mean British Telecommunications plc, including Openreach, EE and all other BT Group companies.


1.1 Date of Last Update
This is version 1.09, 2018/03/05.

1.2 Distribution List for Notifications
We do not provide a notification service for changes to this document.

1.3 Document Locations
https://www.globalservices.bt.com/static/assets/rfc2350/RFC2350-BTCERT.pdf

1.4 Authenticating this Document
Not provided at this time.

2. Contact Information

2.1 Name of the Team

Official Name: British Telecommunications CERT Co-ordination Centre

Short Name: BTCERTCC

2.2 Address

BTCERTCC
pp 302
Sevenoaks Workstyle
160 London Road
Sevenoaks
KENT
TN13 1BT

2.3 Time Zone
We use GMT (UTC +00:00) or BST (UTC +01:00) at different times of year. Please see the following site for the dates when our time-zone changes: https://www.gov.uk/when-do-the-clocks-change

2.4 Telephone Number
+44 20 7388 3354 (Select Option 1 and ask for BTCERTCC, A.K.A. the Third Line Team)

2.5 Facsimile Number
+44 1908 860800 (this is a fax to email service number, messages are automatically converted to email and delivered to btcertcc@bt.com. Please do not use it for sensitive communication)

2.6 Other Telecommunication
None.

2.7 Electronic Mail Address
<btcertcc@bt.com> this is our mailbox address. We monitor it between 09:00 to 17:00 U.K. local time Monday to Friday except weekends and U.K. public holidays. Outside these times, we send an automated response email explaining how to get help.

2.8 Public Keys and Other Encryption Information
For the secure exchange of information with us, our PGP key details are as follows. The public key block is available at https://www.first.org/members/teams/btcertcc

    User ID: BTCERTCC <btcertcc@bt.com>
    Key ID: 0xC91248FE Key type: RSA
    Key size: 2048 Expires: never
    Fingerprint: 362A AE97 370B EE37 94B7 8395 5070 E7A9 C912 48FE

2.9 Team Members
We list our team members on our team registrations at trusted-introducer.org and first.org.

2.10 Other Information
Please see our registrations at trusted-introducer.org and first.org.

2.11 Points of Customer Contact
We prefer external people to contact us using our e-mail address, see section 2.7. Alternatively, our First Line Team provide telephone cover around the clock, including evenings, weekends and public holidays. They answer the telephone number listed in section 2.4.

BT people must report security incidents using the contacts published on our internal BT Security website. For anything else, contact us using our e-mail address, see section 2.7

3. Charter

3.1 Mission Statement
We, BTCERTCC, are part of BT Security Operations. Their role is to protect BT Group, our customers and our people from security threats, wherever they may be in the world.
We hunt for and react to cyber security threats, always looking to improve our capability to do these things. We support the community through our participation in and membership of FIRST and TF-CSIRT.

3.2 Constituency
Our constituency is BT’s own-use computer systems and networks, and where contractually obliged those of our customers.

3.3 Sponsorship and/or Affiliation
British Telecommunications plc, wholly owns BTCERTCC
Registered office: 81 Newgate Street London EC1A 7AJ
Registered in England no: 1800000

3.4 Authority
The BT Security Leadership Team (SLT) provide the authority for us to operate.

We work cooperatively with system administrators and users of BT’s networks and systems. BT Security policies, specifications and standards will guide our actions subject at all times to UK law (including regulatory requirements) or that which applies in the jurisdiction. We will appeal to the SLT to exert its authority, directly or indirectly, should circumstances warrant it.

Where there is customer involvement then we consult BT’s terms of service and we may pass the matter to the relevant BT Customer Service or Customer Security Team for resolution.

4. Policies

4.1 Types of Incidents and Level of Support
BT Security Operations has the authority to investigate all types of computer and network security incidents, which occur or threaten to occur on the BT estate. We provide varying levels of support to them, depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and our resources at the time. The relevant contracts and terms of service apply to the products and services offered by BT.

Whilst we may not be in a position to do so in all cases, if we are able to offer assistance, our team will work with the incident reporter to find an appropriate resolution to the problem. We understand the system administrator community may comprise people with varying expertise. When they call for help, we may give individuals reasonable assistance, balanced against our available resources at that time. However, we cannot provide training or system maintenance on their behalf. In most cases, we will provide pointers to the information needed to implement appropriate measures.

We do not generally provide direct support to end users. They should contact their system administrator or network administrator for assistance in the first instance.

We are committed to keeping BT’s computer and network administration community informed of potential vulnerabilities through our Vulnerability Management process. Our aim is to notify before exploitation of a vulnerability occurs.

4.2 Co-operation, Interaction and Disclosure of Information
We will treat as confidential all information you may disclose to us. Please ensure that you have the legal right to make any such disclosures of information before doing so. If you disclose sensitive
information to us please make this explicitly clear. For example, you could use a generally recognised information classification label in the message title or subject line. We expect BT people to follow BT’s own information classification Policy, which they are able to access from the BT Security intranet site.

For external people we support the Information Sharing Traffic Light Protocol (ISTLP) for classifying information and we manage ISTLP marked information appropriately. For ISTLP see: https://www.first.org/tp/docs/tpv1.pdf.

We recommend the use of PGP encryption for confidential email.

We only distribute information on a need-to-know basis, and preferably in an anonymised form. BT is a global company and we comply with the law in the jurisdiction in which our constituency is operating. This will generally be the U.K. and all relevant U.K. Data Protection Laws apply. Where you report criminal intent to us, we may securely pass the relevant information to the correct authorities.

4.3 Communication and Authentication

When communicating with external people we may use email with a PGP signature, especially if we need to authenticate with them. For internal communications, we may use Secure Mail available from our Messaging Team. We may use telephone communication where you provide an email invitation with your contact information. Alternatively, you may call our First Line Team; see section 2.4, leaving your contact information and asking us to call you. We will attempt to verify your telephone number prior to calling you back so a published number is preferred, for example one registered with the Trusted Introducer or FIRST.org. Please note we do not have encrypted voice communication facilities.

If you need to share sensitive data with us via a network file transfer please encrypt the data before transmission. We use WinZip with AES encryption.

5. Services

5.1 Incident Response

We manage incident response, including triage, coordination and resolution, through our end-to-end Incident Management Process. Where we have agreed to, we will assist system administrators in handling the technical and some organizational aspects of incidents in line with our process. To make use of our incident response services, please refer to section 2.11 above. Please remember that the amount of assistance available will vary according to what we say in section 4.1.

5.2 Incident Triage

See 5.1

5.3 Incident Coordination

See 5.1

5.4 Incident resolution

See 5.1

5.5 Proactive Activities

We participate in a number of proactive initiatives adapting as the threat landscape changes and as resource allows. These may include:

- Threat hunting
- Malware research
Security tools development
Mobile app authentication
Purple teaming

6. Incident Reporting Forms
There are no local forms developed for reporting incidents

7. Disclaimers
While we have taken every precaution in the preparation of information, notifications and alerts, we assume no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.