UNIVERSITY OF CAMBRIDGE
Information Services

RFC 2350 (BCP 21)
Description of University of Cambridge Computer Emergency Response Team (CamCERT)

Author: *Kieren Niĉolas Lovell*
Originator: *Kieren Niĉolas Lovell*
Releasing Officer: Ian Leslie
Senior Information Risk Officer - University of Cambridge

1. Document Information

   1.1. Version Number and Date of last Update

   1.0 – 2017-06-22

   1.2. Distribution Lists

   - Within Security Operations Manual (SOC) held at PARA 2.2.
   - This document is kept up to date in the URL within PARA 1.3.

   1.3. Available at www.uis.cam.ac.uk/cambridge-cert-contact

2. Contact Information

   2.1. Team Name

   Full Name: University of Cambridge Incident Response (UIS) Team
   Short Name: CamCERT

   2.2. Address

   Incident Response (UIS) Team
   Security Operations Centre
   Roger Needham Building
   Cambridge
   CB3 0RH
   United Kingdom

   2.3. Timezone

   GMT/UTC (GMT/UTC+0100 in Summer Time)

   2.4. Telephone Number

   +447523 500538 (Duty CERT) (Primary Contact)

   +441223 911574 (Head of CERT)

   2.5. Facsimile Number

   N/A

   2.6. Other Telecommunications Available on Request

   Skype (Duty CERT: Live:787a27e1c89f2e09)

   2.7. Electronic Mail Address

cert [AT] cam . ac . uk – Emails are monitored 24 hours a day.

Fallback Email – In the event that we cannot use our email system, the following email address is used as an emergency email system:

CERTCambridge [at] gmail.com

2.8. Public Keys and Encryption Information

The following details are for sending encrypted information to the Head of CERT only. This account is not monitored 24/7. For the Duty CERT's key details, make a request via a plain text email requesting the public key in the subject line. (PARA 2.4 & 2.7 refers).

BDOC files can be transmitted via kieren.nicolas.lovell [at] eesti.ee

PGP: kml52 [at] cam.ac.uk (Key available at www.lovell.ee/pgp-key)

Fingerprint: B0BA 08EE 0967 860C 433C 572C 73B4 2A78 7D16 B30E

2.9. Team Members

Head of CamCERT is Mr Kieren Niĉolas Lovell.

Skype: kieren.nicolas.lovell [at] eesti.ee | Jabber/XMPP: Kieren [at] jabbim.sk (PGP Available on Jabber – Key the same as PARA 2.8).

Information about other team members is not held within this document.

2.10. Points of Customer Contact

Email (PARA 2.7) is the preferred method of contact.

If the material you are transmitting is of a sensitive nature, please transmit via encrypted communication channels. Details of available systems and keys are located in PARA 2.8 or via Skype (Details in PARA 2.6)

@UniCamInfoSec is the CamCERT Twitter account.

3. Charter

3.1. Mission Statement

CamCERT's mission is to support all members, students, staff, College and Institutions in the University of Cambridge against intentional and malicious activities that would hamper the integrity, availability &/or confidentiality of their IT assets, or cause harm to other institutions or people.

CamCERT will operate in accordance with the following key values:

- Highest standards of ethical integrity
- Provide a high level of operational readiness, with the ability to activate a rapid reaction tiger team and a silver team, during major incidents.
- Dealing effectively with incidents in a timely fashion
- Leading by example with good communications and security practices
- Fostering a culture of information exchange between other CERT/CSIRT organisations, whilst operating on a ‘Need to Know' basis.

3.2. Constituency

The main areas of responsibility of CamCERT are:

- Dealing with Information Security incidents that are within the CUDN (Cambridge University Data Network)
- Serving as a single point of contact for national and foreign CERTs/CSIRTs
- Co-ordinating the response in case of incident escalation.
- Educating the community and IT sector within Cambridge on cyber threats, and providing Cyber Security reports and situational awareness training, where and when required.

3.3. Sponsorship and/or Affiliation

CamCERT is a sub department from the University of Cambridge Information Services division. We are endorsed by the Information Services Committee of the University of Cambridge. We act as the SPOC for JISC CSIRT for matters relating to the University of Cambridge and we work with other Legal Enforcement Agencies.

3.4. Authority

CamCERT has the authority to act on all incidents that cause, or could cause, detriment to the confidentiality, integrity and availability of Cambridge University IT assets.

4. Policies

4.1. Types of Incident & Levels of Support

4.1.1. Types of Incident

Root Level Intrusion (Incident) – CAT 1

Privileged access on a Computer system or network that is unauthorised. Privileged access (which can be referred to as admin or root access) provides unrestricted access to the system. This level includes unauthorised access to data or information that has been obtained by access using someone’s account

credentials. IT systems that have been compromised with malicious code, that provide remote interactive control, will also be reported as this classification.

User Level Intrusion (Incident) – CAT 2

This type of Intrusion relates to an unauthorised system/network access to a non-privileged account on an IT system. Non-privileged access, often referred to as 'User Level' access, will provide the aggressor with restricted access to an IT system. This will include authorised access to information, and use of the credentials to gain access to other personal information or access permissions (For example; Employee self-service, Hermes email, User Network shares). If any malicious code is activated that provides the aggressor with remote interactive control of this user security level, it will be reported with this classification.

Unsuccessful Activity Attempt (Event) – CAT 3

This classification covers deliberate attempts to gain unauthorised access to an IS system, that are defeated by our normal defensive security posture. The attacker fails to gain any access (User or Root) and the activity does not have the characteristics as exploratory scanning of our network. Reporting of these types of events is critical for intelligence gathering in order for us to produce effects-based metrics for our Threat Assessment reports. This classification, however does not cover “drive by” virus injections that are defeated/neutralised by our AV solutions. “Run of the mill” malware injections that are immediately defeated by AV solutions are not reported as a threat level, and are included in “Drive-by Malware” classification.

Denial of Service (Incident) – CAT 4

An activity that denies, degrades or disrupts normal operations of the University infrastructure, and affects the normal operations of the University.

Non-Compliance Activity (Event) – CAT 5

Activity that potentially exposes the University of Cambridge's Information Security posture as a result of action, or inaction, of authorised users. This includes administrative and user actions, such as failure to update software packages with the latest security patches, misconfiguration firewalls, installation of vulnerable programs, and other breaches to the ISC Policy. Reporting of this classification is critical for UIS to mitigate any threats on our network before they become attack vectors used by threat actors.

Reconnaissance (Event) – CAT 6

Activity that seeks to gather information used by our IT systems, applications, information held on our servers, and information about our users that may be useful in formulating an attack profile. This activity includes mapping our network (Port scanning), interconnectivity, SQL mapping (For further attacks), and social engineering campaigns, designed to extract information that could be used for a further exploitation of our network. This activity does not directly mean there has been a compromise, but that the importance of acting upon this information means we directly mitigate any possible threat.

Malicious Logic (Incident) – CAT 7

This classification of incident is software that is designed and/or deployed by threat aggressors with malicious intentions for the purposes of gaining access to information without the consent of the user. This only includes malicious code that does not provide remote interactivity control of the compromised account. Malicious code that has allowed interactive access should be classified in either Root Level or User Level.

Investigating (Event) – CAT 8

This classification covers incidents or malicious or anomalous activity deemed suspicious and warrant further investigation, and will require investigation and re-classification upon further review.

Explained Anomaly (Event) – CAT 9

Suspicious events that, upon further investigation, are determined to be non-malicious activity and do not fit the normal classification framework. This includes Infrastructure malfunctions and false alarms. When reporting these incidents, they will be given a caveat with a clear, concise reason of why they are classified as in this category.

4.1.2. Levels of Support/Response Times

Incident information that is received by CERT is parsed, logged, & forwarded to various relevant Computer Officers across the CUDN. The level of support provided by CamCERT depends on the type, severity, and the impact the incident causes the University of Cambridge critical infrastructure. Communications are in place that allow escalation of matters to key stakeholders within the IT estate. All enquires will be handled accordingly as they are assessed on their level of impact. The following handling times will be how we deal with an incident, and are identified by the following tag:

Prosign / Full Title / Timeframe

Z / FLASH / ASAP
O / Immediate / 30 minutes – 1 Hour
P / Priority / 1 Hour – Six Hours
R / Routine / Six Hours - Start of the Next working day

4.1.3. Policies, rules and guidelines in detail are provided here:

http://www.uis.cam.ac.uk/about-us/governance/uis-policies-and-guidelines

4.2. CamCERT works closely with UK and EU institutions & law enforcement agencies. All relevant UK Data Protection Laws apply. In the case of criminal intent, these will be past on securely to the correct authorities.

Any case studies generated and disseminated in professional settings will be in an anonymous form.

4.3. Communications and Authentication

For international communications – Communications should be first established using only trusted and listed teams (TI) and by using PGP or S/MIME.

5. Services

5.1. Incident Response

CamCERT will define, assess and prioritise all types of ICT incidents in precedence order (in accordance with the handling times and tags contained within PARA 4.1). CamCERT will provide Incident Triage, Incident Co-ordination, and Incident Resolution. The following impact assessments are used by CamCERT.

None

The incident is routine, and has no adverse affects on the University. The incident contains no loss of CIA (Confidentiality, Availability & Integrity), and no loss of PI data. The incident is still reported, but has no operational impact on the University.

Low

The impact is assessed as low if the loss of CIA is expected to have a limited adverse effect on the University's operations, information assets, or individuals. This classification is given to an incident on the following conditions;
A. Cause degradation in the ability of University to carry out it's operational functions. The University can still perform its primary objectives and functions.
B. Result in minor damage to our IT/Information Assets
C. Result in minor loss (Financially) and/or might result in minor harm to individuals.

Moderate

A potential loss of confidentiality, integrity and availability is expected, and could have serious adverse effects on the operational functions of the University, our Information Assets, and individuals.
A. Cause serious degradation in the ability of University to carry out it's operational functions. The University activates fall backs to perform standing operations, but maintains operating at a required level.
B. Serious loss to IT/Information Assets that require immediate notification to authorities
C. Result in significant financial loss.
D. Results in significant harm to people within or connected to the University, but does not involve loss of life or serious life threatening injuries.

High

The impact is classified as high if the loss regarding CIA is, or is expected, to have severe or catastrophic effects on the University's operations, Information Assets, and/or Individuals.
A. Cause severe degradation to services and the University loses the ability to perform one of it's primary functions, as a result of the incident/event.
B. Major damage/loss to IT/Information Assets
C. Major Financial Loss
D. Results in severe or catastrophic harm to a number of individuals involving loss of life, or serious life threatening injuries.

5.2. Proactive Activities

Provide relevant information on threats, trends, and remedies to our constituency (and international communications) to raise security awareness and competence.

Collecting and maintaining communications details for information security teams.

Community building and information exchange within the constituency.

6. Incident Reporting Forms

https://help.uis.cam.ac.uk/user-accounts-security/information-management/incident-reporting

7. Disclaimers

While every precaution will be taken in preparation & dissemination of information and security alerts, CamCERT assumes no responsibility to external (Non-University of Cambridge organisations and users) for errors, omissions, or for damages resulting from the use of the information provided within this document or our security communications.