WAGENINGEN
UNIVERSITY & RESEARCH

Charter Wageningen University and Research CERT

RFC 2350

DATE
May 22, 2019

AUTHOR
Remon Klein Tank

VERSION
v2.3

STATUS
final

WUR (Wageningen University and various research institutes) is specialised in the domain of healthy food and living environment.

Table of contents

1 About this document

1.1 Date of Last Update

This is version was updated and published on the 22nd of May 2019. It was approved by the leiderschapsteam FB-IT.

1.2 Distribution List for Notifications

Notifications of updates are submitted to our mailing list cert-info@wur.nl. Subscription requests for this list should be sent to the Servicedesk at servicedesk.it@wur.nl.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the CERT website; its URL is https://cert.wur.nl/. Please make sure you are using the latest version.

1.4 Authenticating this Document

This document is been signed with the WUR-CERT PGP key. The signature is available on our website: https://cert.wur.nl/.

2 Contact Information

2.1 Name of the Team

"WUR-CERT": The Wageningen University and Research center Computer Emergency Response Team.

2.2 Address

Wageningen University and Research
WUR-CERT
Akkermaalsbos 12
6708WB Wageningen
The Netherlands

2.3 Time Zone

CET/CEST (GMT+01:00, and GMT+02:00 from April to October). See 2.11 for business hours.

2.4 Telephone Number

During business hours the CERT can be reached through the WUR-Servicedesk at: +31 317 488888 (ask for the WUR-CERT). Regular business hours are from 08:30-17:00 from Monday to Friday except public holidays in the Netherlands.

2.5 Other Telecommunication

Mobile phone numbers of the members of the CERT team will be made available to the WUR Servicedesk, the administrators of the WUR infrastructure team participating in the consignment service and the SURFCert team. These numbers can be called at all times but should be used for emergencies only.

2.6 Electronic Mail Address

The WUR-CERT can be reached through email by cert@wur.nl and abuse@wur.nl. This is a mailbox witch will be checked regularly during business hours by the person(s) on duty for the WUR-CERT. Outside the business hours, the mailbox will be checked on best-effort principle with reasonable intervals.

2.7 Public Keys and Other Encryption Information

The WUR-CERT has a PGP key, whose KeyID is published on https://cert.wur.nl. The key and its signatures can be found at the usual large public keyservers.

2.8 Team Members

The roles of the WUR-CERT coordinator and liaison officer are assigned to the team member on duty at that time. Backup coordinators and other team members, along with their areas of expertise and contact information, are listed at the WUR-CERT website.

2.9 Other Information

General information about the WUR-CERT can be found at the WUR-CERT website.

2.10 Points of Customer Contact

In case of a security incident the preferred method for contacting the WUR-CERT is via e-mail at cert@wur.nl. All other non-critical questions and remarks should be sent to the Servicedesk at servicedesk.it@wur.nl.

If it is not possible (or not advisable for security reasons) to use e-mail, the WUR-CERT can be reached by telephone during regular office hours. The WUR-CERT's hours of operation are generally restricted to regular business hours (08:30-17:00 from Monday to Friday except public holidays in the Netherlands).

3 Charter

3.1 Mission Statement

The purpose of the WUR-CERT is to respond to computer security incidents that occur on the WURnet.

For the world, WUR-CERT is the WUR interface with regards to IT security incident response. All IT security incidents related to the WURnet can be reported to WUR-CERT.

3.2 Constituency / Affiliation

All users of the WUR network (WURnet), as defined in the context of the "*WUR Regulations for Network*". This policy is available at the WUR internet or intranet site.

3.3 Sponsorship and/or Affiliation

The WUR-CERT is part of the WUR FB-IT department.

3.4 Authority

The WUR-CERT operates under the auspices of, and with authority delegated by, the Executive Board of Wageningen University and Research. For further information on the mandate and authority of the FB IT department, please refer to the "*WUR Regulations for Network* ". This document is available on request and/or can be found on the WUR intranet/internet.

The WUR-CERT expects to work cooperatively with system administrators and users at WUR, and, insofar as possible, to avoid authoritarian relationships. However, should circumstances warrant it, the WUR-CERT will appeal to users or administrators to exert its authority, direct or indirect, as necessary. Some members of the WUR-CERT are administrators of the WUR domain, and have all of the powers and responsibilities assigned to Systems Administrators by the WUR Regulations for Network, or have the security officer role.

Users of the WURnet network who wish to appeal the actions of the WUR-CERT should contact the Security officer. If this recourse is not satisfactory, the matter may be referred to the head of FB-IT.

4 Policies

4.1 Types of Incidents and Level of Support

The WUR-CERT is authorized to address all types of computer security incidents which occur, or threaten to occur, at the WUR.

The level of support given by WUR-CERT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the WUR-CERT's resources at the time, though in all cases some response will be made within one working day.
Resources will be assigned according to the following priorities, listed in decreasing order:

- Threats to the physical safety of human beings.
- Root or system-level attacks on any Management Information System, or any part of the backbone network infrastructure.
- Root or system-level attacks on any large public service machine, either multi-user or dedicated-purpose.
- Compromise of restricted confidential service accounts or software installations, in particular those used for MIS applications containing confidential data, or those used for system administration.
- Denial of service attacks on any of the above three items.
- Any of the above at other sites, originating from WURnet.
- Large-scale attacks of any kind, e.g. sniffing attacks, IRC "social engineering" attacks, password cracking attacks.
- Threats, harassment, and other criminal offenses involving individual user accounts.
- Compromise of individual user accounts on multi-user systems.
- Compromise of desktop systems.
- Forgery and misrepresentation, and other security-related violations of local rules and regulations, e.g. usenet news and e-mail forgery, unauthorized use of IRC bots.
- Denial of service on individual user accounts, e.g. mailbombing.

Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent. Note that no direct support will be given to end users; they are expected to contact their Servicedesk or local support for assistance. The WUR-CERT will support the latter people.

While the WUR-CERT understands that there exists great variation in the level of system administrator expertise at the WUR, and while the WUR-CERT will endeavour to present information and assistance at a level appropriate to each person, the WUR-CERT cannot train system administrators on the fly, and it cannot perform system maintenance on their behalf.

In most cases, the WUR-CERT will provide pointers to the information needed to implement appropriate measures.

The WUR-CERT is committed to keeping the WUR system administration community informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

While there are legal and ethical restrictions on the flow of information from WUR-CERT, many of which are also outlined in the WUR Regulations for Network, and all of which will be respected, the WUR-CERT acknowledges its indebtedness to, and declares its intention to contribute to, the spirit of cooperation that created the Internet. Therefore, while appropriate measures will be taken to protect the identity of members of our constituency and members of neighbouring sites where necessary, the WUR-CERT will

otherwise share information freely when this will assist others in resolving or preventing security incidents.

In the paragraphs below, "affected parties" refers to the legitimate owners, operators, and users of the relevant computing facilities. It does not refer to unauthorized users, including otherwise authorized users making unauthorized use of a facility; such intruders may have no expectation of confidentiality from the WUR-CERT. They may or may not have legal rights to confidentiality; such rights will of course be respected where they exist.

Information being considered for release will be classified as follows:

- Private user information is information about particular users, or in some cases, particular applications, which must be considered confidential for legal, contractual, and/or ethical reasons.
    - Private user information will be not be released in identifiable form outside the WUR-CERT, except as provided for below. If the identity of the user is disguised, then the information can be released freely (for example to show a sample user registry file as modified by an intruder, or to demonstrate a particular social engineering attack).
- Intruder information is similar to private user information, but concerns intruders.
    - While intruder information, and in particular identifying information, will not be released to the public (unless it becomes a matter of public record, for example because criminal charges have been laid), it will be exchanged freely with system administrators and CERTs tracking an incident.
- Private site information is technical information about particular systems or sites.
    - It will not be released without the permission of the site owner in question, except as provided for below.
- Vulnerability information is technical information about vulnerabilities or attacks, including fixes and workarounds.
    - Vulnerability information will be released freely, though every effort will be made to inform the relevant vendor before the general public is informed.
- Embarrassing information includes the statement that an incident has occurred, and information about its extent or severity. Embarrassing information may concern a site or a particular user or group of users.
    - Embarrassing information will not be released without the permission of the site or users in question, except as provided for below.
- Statistical information is embarrassing information with the identifying information stripped off.
    - Statistical information will be released at the discretion of FB-IT.
- Contact information explains how to reach system administrators and CERTs.
    - Contact information will be released freely, except where the contact person or entity has requested that this not be the case, or where WUR-CERT has reason to believe that the dissemination of this information would not be appreciated.

Potential recipients of information from the WUR-CERT will be classified as follows.

- Because of the nature of their responsibilities and consequent expectations of confidentiality, members of WUR-CERT team are entitled to receive whatever information is necessary to facilitate the handling of computer security incidents which occur in their jurisdictions.

- Members of the Personnel Council are entitled to receive whatever information they request concerning a computer security incident or related matter which has been referred to them for resolution.

- System administrators at WUR are also, by virtue of their responsibilities, trusted with confidential information. However, unless such people are also members of WUR-CERT, they will

be given only that confidential information which they must have in order to assist with an investigation, or in order to secure their own systems.

- Users at WUR are entitled to information which pertains to the security of their own computer accounts, even if this means revealing "intruder information", or "embarrassing information" about another user. For example, if account aaaa is cracked and the intruder attacks account bbbb, user bbbb is entitled to know that aaaa was cracked, and how the attack on the bbbb account was executed. User bbbb is also entitled, if she or he requests it, to information about account aaaa which might enable bbbb to investigate the attack. For example, if bbbb was attacked by someone remotely connected to aaaa, bbbb should be told the provenance of the connections to aaaa, even though this information would ordinarily be considered private to aaaa. Users at the WUR are entitled to be notified if their account is believed to have been compromised.

- The WUR community will receive no restricted information, except where the affected parties have given permission for the information to be disseminated. Statistical information may be made available to the general WUR community. There is no obligation on the part of the WUR-CERT to report incidents to the community, though it may choose to do so; in particular, it is likely that the WUR-CERT will inform all affected parties of the ways in which they were affected, or will encourage the affected site to do so.

- The public at large will receive no restricted information. In fact, no particular effort will be made to communicate with the public at large, though the WUR-CERT recognizes that, for all intents and purposes, information made available to the WUR community is in effect made available to the community at large, and will tailor the information in consequence.

- The computer security community will be treated the same way the general public is treated. While members of WUR-CERT may participate in discussions within the computer security community, such as newsgroups, mailing lists (including the full-disclosure list "bugtraq"), and conferences, they will treat such forums as though they were the public at large. While technical issues (including vulnerabilities) may be discussed to any level of detail, any examples taken from WUR-CERT experience will be disguised to avoid identifying the affected parties.

- The press will also be considered as part of the general public. The WUR-CERT will not interact directly with the Press concerning computer security incidents, except to point them toward information already released to the general public. If necessary, information will be provided to the WUR Communication Services department, and to the Servicedesk of FB-IT. All incident-related queries will be referred to these two bodies. The above does not affect the ability of members of WUR-CERT to grant interviews on general computer security topics; in fact, they are encouraged to do to, as a public service to the community.

- The SURF trusted community of well-known CERTS, SCIRT, will in some cases be trusted with confidential information. This will happen only if the information transmitted will be limited to that which is likely to be helpful in identifying or resolving a potential incident.

- Governmental parties as NCSC will in some cases be trusted with confidential information. Information transmitted will be limited to that which is likely to be helpful in resolving the incident.

- For the purposes of resolving a security incident, otherwise semi-private but relatively harmless user information such as the provenance of connections to user accounts will not be considered highly sensitive, and can be transmitted to a foreign site without excessive precautions. "Intruder information" will be transmitted freely to other system administrators and CSIRTs.

"Embarrassing information" can be transmitted when there is reasonable assurance that it will remain confidential, and when it is necessary to resolve an incident.

- Vendors will be considered as foreign CSIRTs for most intents and purposes. The WUR-CERT wishes to encourage vendors of all kinds of networking and computer equipment, software, and services to improve the security of their products. In aid of this, a vulnerability discovered in such a product will be reported to its vendor, along with all technical details needed to identify and fix the problem. Identifying details will not be given to the vendor without the permission of the affected parties.

- Law enforcement officers will receive full cooperation from the WUR-CERT, including any information they require to pursue an investigation, in accordance with the WUR Regulations for Network and Dutch law.

4.3 Communication and Authentication

In view of the types of information that the WUR-CERT will likely be dealing with, voice calls will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail or messaging will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send sensitive data end to end encryption is required. For e-mail, PGP will be used, messaging is restricted to verified Signal or Threema accounts. Network file transfers outside of the WUR will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted prior to transmission, preferably with SURF filesender, using SMS or messenger to send the encryption key. Sensitive information is preferably stored encrypted on the WUR-CERT fileshare.

Where it is necessary to establish trust, for example before relying on information given to the WUR-CERT, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within WUR, and with known neighbour sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information, et cetera, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular is supported).

5 Services

5.1 Incident Response

WUR-CERT will assist system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1 Incident Triage

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

5.1.2 Incident Coordination

- Determining the initial cause of the incident (vulnerability exploited).
- Facilitating contact with other sites which may be involved.
- Facilitating contact with appropriate law enforcement officials, if necessary.
- Making reports to other CERTs.

5.1.3 Incident Resolution

- Removing the vulnerability.
- Securing the system from the effects of the incident.
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.
- Collecting evidence where criminal prosecution, or disciplinary action by the WUR is contemplated.

In addition, WUR-CERT will collect statistics concerning incidents which occur within or involve the WUR community, and will notify the community as necessary to assist it in protecting against known attacks.

To make use of WUR-CERT's incident response services, please send e-mail (see above under Electronic Mail Address). Please remember that the amount of assistance available will vary according to the parameters described.

5.2 Proactive Activities

The WUR-CERT coordinates and maintains the following services to the extent possible depending on its resources:

- Information services
  - Regular updates to inform security contacts within a relevant MDT of new information or developments relevant to their IT environments.
- Records of security incidents handled will be kept. While the records will remain confidential, periodic statistical reports can be made available to the WUR community.
- Red teaming to test internal processes and infrastructure

6 Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, WUR-CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.