Dienstbeschrijving SURFcert

SURFcert Service Description (RFC 2350)

Below, you will find the SURFcert Service Description, which states, among other things, the services that SURFcert provides.

Author/Source: Wim Biemolt
Distribution: World
Classification : Unclassified External
Subject : RFC 2350 formatted SURFcert Service Description
Index : R-16-01
Page : 1
Version : 7
Date: 19-09-2023

1. About this document

1.1 Date of last update

This is version 7, published 19 September 2023.

1.2 Distribution List for Notifications

Notifications of updates are submitted to our mailing list. Site Security Contacts of SURF customers are automatically added to this list. Subscription to this list is limited to Site Security Contacts of SURF customers. Only SURFcert can post messages to this list.

1.3 Locations where this document may be found

The current version of this CSIRT description document is available from the SURFcert wiki site; its URL is https://wiki.surfnet.nl/display/SURFcert/Dienstbeschrijving+SURFcert. Please make sure you are using the latest version.

1.4 Authenticating this document

Currently, no PGP-signed version of this document is available.

2. Contact information

2.1 Name of the team

"SURFcert": the SURF Computer Emergency Response Team.

2.2 Address

Visiting address

SURFcert
Hoog Overborch
Moreelsepark 48
3511 EP Utrecht
the Netherlands

Post address

SURFcert
P.O. Box 19035
3501 DA Utrecht
the Netherlands

2.3 Time zone

UTC+0100 in winter and UTC+0200 in summer (DST). Daylight savings time is according to EC rules, central European time.

2.4 Telephone number

+31 622923564, outside business hours emergencies only, attended at all times.

2.5 Facsmile number

Not available.

2.6 Other telecommunications

None available.

2.7 Electronic Mail Address

cert [at] surfcert.nl; This is a mail alias that relays mail to all SURFcert kernel members. There is always one kernel member on duty. This kernel member handles all incoming mail.

2.8 Pubic keys and other encryption information

SURFcert uses PGP for encryption and signing. The PGP key can be found on the PGP-keyserver: https://keys.openpgp.org/search?q=cert@surfcert.nl.

2.9 Team members

SURFcert consists of 10 members; currently 6 from SURF and 4 for the connected institutions:

- Wim Biemolt (SURFcert chair).
- Paul Dekkers
- Jaap van Ginkel (UvA)
- Jeffeny Hoogervorst
- Koos van den Hout (UU)
- Thijs Kinkhorst
- Remon Klein Tank (WUR)
- Melvin Koelewijn
- Luuk Oostenbrink
- Peter Peters (UT)

2.10 Other information

General information about SURFcert can be found at https://surf.nl/surfcert.

2.11 Points of customer contact

The preferred method for contacting SURFcert is via e-mail at ; e-mail sent to this address will be acted upon by the officer on duty. Response time for normal priority is within 1 working day.

If it is not possible (or not advisable for security reasons) to use e-mail, SURFcert can be reached by telephone during regular office hours.

Normal SURFcert service hours are 09:00 until 17:00 on working days (except on public holidays). In case of a real emergency SURFcert has a 24/7 attended emergency phone number (please check 2.4).

3. Charter

SURFcert operates under a charter. This charter can be found at: R--92--01 Operational Framework SURF certDetails on SURFcert operation can be found in this operational framework.

3.1 Mission statement

The primary purpose of SURFcert is to provide a mechanism for institutions within the Netherlands, connected to SURF, to deal with computer security problems and their prevention.

The goals of SURFcert are:

- To handle security incidents and solve security problems (assist where necessary).
- To educate in a general sense (give general recommendations to system managers and users, by means of information distribution).

3.2 Constituency

The SURFcert Constituency are those sites that are connected to SURF.

3.3 Sponsorship and/or affiliation

SURF bv will fund the work of SURFcert and will fund the technical provisions needed in order to gain and maintain maximum reachability.

SURFcert is affiliated with FIRST (http://www.first.org), the Forum on Incident Response and Security Teams and maintains affiliations with various other CSIRTs around the world on an as needed basis. SURFcert is also Trusted Introducer Certified team

3.4 Authority

SURFcert operates under the auspices of, and with authority delegated by, the directors of SURF bv.

SURFcert expects to work cooperatively with system administrators, networkmanagers and users of SURF connected institutions, and, insofar as possible, to avoid authoritarian relationships. However, should circumstances warrant it, SURFcert has the authority to take the measures it deems appropriate to properly handle a computer security related incident.

SURF connected institutions who wish to appeal the actions of SURFcert should contact the SURFcert chair, Wim Biemolt.

If this recourse is not satisfactory, the matter may be referred to the SURF director through your SURF account manager.

4. Policies

4.1 Types of incident and level of support

SURFcert is authorized to address all types of computer security incidents which occur, or threaten to occur, at its constituency (see 3.2). SURFcert may act upon request of one of its constituents, or may act if a constituent is, or threatens to be, involved in a computer security incident.

The level of support given by SURFcert will vary depending on the type and severity of the incident or issue, the size of the user community affected, and the SURFcert'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:

1. Threats to the physical or mental safety of human beings.
2. Root or system-level attacks on any Server System, or any part of the backbone network infrastructure.
3. Root or system-level attacks on any large public service machine, either multi-user or dedicated-purpose.
4. Any other type of compromise which leads or may lead to unauthorised access of systems.
5. Denial of service attacks on any of the above three items.
6. Any of the above at other sites, originating from the constituency of SURFcert.
7. Large-scale attacks of any kind, e.g. sniffing attacks, IRC "social engineering" attacks, password cracking attacks.

8. Threats, harassment, and other criminal offenses involving individual user accounts.
9. Compromise of desktop systems.
10. 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. These incidents will be assessed as to their relative severity at SURFcert's discretion.

SURFcert will, in principle, accept any incident report that involves an incident with one of the constituents either as a victim or as a suspect. Henceforth, reports filed by individual end users within the constituency will also be dealt with. However, SURFcert encourages the engagement of qualified security staff at the involved organisation in an early stage. Whenever feasible, SURFcert will contact the relevant Site Security Contact or the Security Entry Point of the organisation alledgedly involved, even if the end user has chosen not to do so.

While SURFcert understands that there exists great variation in the level of system administrator expertise at its constituency, and while SURFcert will endeavor to present information and assistance at a level appropriate to each person, SURFcert shall not train system administrators on the fly, and it cannot perform system maintenance on their behalf. In most cases, SURFcert will provide pointers to the information needed to implement appropriate measures.

SURF, as the organisation under whose sole jurisdiction SURFcert is operating, offers the possibility to the constituency for consultancy projects on an ad-hoc basis. In security related matters, SURFcert may at its own discretion suggest to embark on a consultancy project, which will provide for more resources where necessary in order to do a full analysis and remedial of an observed security breach.

4.2 Co-operation, interaction and disclose of information

While there are legal and ethical restrictions on the flow of information from SURFcert, all of which may also be outlined in policies at the organisations of its constituency, and all of which will be respected, SURFcert 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, SURFcert 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 SURFcert. They may or may not have legal rights to confidentiality; such rights will of course be respected where they exist. SURFcert may release information to any third party or to governing authorities whenever there is a legal obligation to do so. However, SURFcert may in some cases delay this action until such a circumstance has been established irrevocably, e.g. by court order. SURFcert will in such cases always notify the affected persons or organisations.

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 SURFcert, 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 .cshrc 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 CSIRTs 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 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 SURFcert.
- Contact information explains how to reach system administrators and CSIRTs.

  Contact information will be released freely, except where the contact person or entity has requested that this not be the case, or where SURFcert has reason to believe that the dissemination of this information would not be appreciated.

Potential recipients of information from SURFcert will be classified as follows:

- Because of the nature of their responsibilities and consequent expectations of confidentiality, members of the constituency's management are entitled to receive whatever information is necessary to facilitate the handling of computer security incidents which occur in their jurisdictions.
- System administrators at organisations that are members of the constituency are also, by virtue of their responsibilities, trusted with confidential information. However, unless such people are also members of SURFcert, 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 within the constituency 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 they request 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 within the constituency are entitled to be notified if their account is believed to have been compromised.
- The constituency 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 community. There is no obligation on the part of SURFcert to report incidents to the community, though it may choose to do so; in particular, it is likely that SURFcert 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 SURFcert recognizes that, for all intents and purposes, information made available to its constituency 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 SURFcert 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 SURFcert experience will be disguised to avoid identifying the affected parties.
- The press will also be considered as part of the general public. SURFcert will generally not interact directly with the Press concerning computer security incidents, except to point them toward information already released to the general public. However, SURFcert acknowledges the role of the Press as a vehicle to inform the broad public in general and its own constityency in particular. To properly accomodate this function, the SURF Public Relations department acts as the focal point in Press contacts. The SURF Public Relations department will call in SURFcert in case a SURFcert statement is needed. Only SURFcert can make statements on behalf of SURFcert. The Chief Information Officer and the Chair are responsible for making public statements on behalf of SURFcert. The above does not affect the ability of individual members of SURFcert to grant interviews on general computer security topics; in fact, they are encouraged to do so, as a public service to the community. Note that all SURFcert members are committed to absolute confidentiality pertaining specific incidents.
- Other sites and CSIRTs, when they are partners in the investigation of a computer security incident, will in some cases be trusted with confidential information. This will happen only if the other site's bona fide can be verified, and the information transmitted will be limited to that which is likely to be helpful in resolving the incident. Such information sharing is most likely to happen in the case of sites well known to SURFcert (for example, several other European CSIRTs have informal but well-established working relationships with SURFcert in such matters).
  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.
  In its contact with other CSIRTs, SURFcert will see to it that the information which is made available to others, will be signed (so as to provide for non-repudiation), and, whenever deemed necessary, crypted. See also 4.3 for more details.
- Vendors will be considered as foreign CSIRTs for most intents and purposes. SURFcert 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 SURFcert, including any information they require to pursue an investigation, notwithstanding the earlier statements made about confidentiality.

4.3 Communication and authentication

In view of the types of information that SURFcert will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted before transmission.

Where it is necessary to establish trust, for example before relying on information given to SURFcert, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within the constituency, 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, etc, 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).

SURFcert keys can be found on https://keys.openpgp.org/search?q=cert@surfcert.nl.

5. Services

5.1 Incident response

SURFcert will assist system administrators in handling the technical and organisational 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

- Assessing whether indeed an incident occured.
- 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 contacts with the affected constituent and/or appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs.
- Composing announcements to users, if applicable.

5.1.3 Incident resolution

SURFcert provides no incident resolution services.

5.2 Proactive activities

SURFcert coordinates and maintains the following services to the extent possible depending on its resources:

- Archiving services
  Records of security incidents handled will be kept. While the records will remain confidential, periodic statistical reports will be made available to the constituency.
- Consultancy services
  On a case-to-case basis, SURFcert may initiate or facilitate projects that are aimed to improve the security of ICT resources at an organisation within the constituency. The feasibility of such projects will be assessed given the severity of the security breach at hand, and the availability of sufficient resources within SURFcert in order to effectively complete the proposed project. If circumstances warrant so, SURFcert may, with the approval of the organisation involved, engage subcontractors for completing the project.

6. Incident reporting forms

It is no longer supported to submit portscan/probe incidents through special forms. All incidents can be reported by any of the in previous chapters mentioned methods.

7. Disclaimers

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