File an incident report

FI | **EN**

How to file an incident report

An incident report can be filed by e-mail, phone or by fax.

In the incident report it is useful to tell briefly what has happened and how. If possible, it is usually good to attach log files that indicate the source- and destination addresses and port numbers.

It is also vitally important to mention the time of the incident. The time zone should also be mentionend, for instance UTC.

When collecting information for the report, be careful not to accidentally temper with the evidence material, i.e. by changing the timestamps. The best thing is to take a disk image of the hard drive and keep the original untouched.

If the report includes confidential information like personal data, system configuration information or security-related information, we recommend using encrypted e-mail communication.

When sending a report by e-mail you will receive an reply as soon as possible depending on the requirements of the incident. Keep the incident number on the subject line if you reply later with more information, this way we can merge it automatically with the original message.

Incident handling is carried out using a special tool, RTIR.

An incident report could look like this:

```
Hi,

There are frequent probes on our web-server
www.example.com, 192.0.43.10
from the address 10.10.10.10.

The probes look like this (timestamps UTC):

Jan 15 10:04:02 example sshd[14523]: Illegal user example from
::ffff:10.10.10.10

The amount of intrusion attemts from 10.10.10.10 is quite high:

www:/var/log# grep 10.10.10.10 auth.log |wc
2359 23592 187184

-> 2359 tries!

Could you help in stopping these attempts.

Aron Admin
```

Remember that the formatting is not crucial when you file a report to Funet CERT; don`t hesitate to write in free form.

Encryption of e-mail messages

If the incident report contains confidential or identity information all e-mail exchange should be encrypted. Funet CERT uses PGP-encryption for confidential messaging.

With PGP you can communicate with Funet CERT using a strong encryption, guaranteeing that only the proper parties have access to the content of the messages.

PGP is based on open and public algorithms and is available free of charge for academic use. GPG is a GNU-licensed free alternative to PGP. Both of them uses so-called public key encryption to encrypt data.

When installing the PGP software the installer will create public and private key pair. The private key should be secured with a strong passphrase and stored in a secure location. You can then share your public key with Funet CERT through a web page or by e-mail. Funet CERT's public key is available on our web page.

When you wish to send an encrypted message to Funet CERT, encrypt it using our public key. This ensures that only Funet CERT personnel can access the message. When we reply, we will encrypt the message using your public key if available.

Criminal offence reports and incidents of abuse

Serious incidents, such as interference with data communication or data breach, should be reported to the police, as well. Primarily these are considered as complainant offences, which means that the reporter itself must file a report to the police. The report can be filed at the local police station, but in more extensive and serious cases it is also possible to contact the National Bureau of Investigation directly.

If the incident is a milder violation against a private user, such as an activity considered disturbing or contrary to the rules, you can also directly contact bodies that monitor incidents of abuse. The address format is abuse@organization. You can also use the whois service provided on, for example the www service of the European RIPE.

Report handling at Funet CERT

You will receive an response to your report when we have registered it and the incident handling has been started.

If necessary, Funet CERT will then contact other parties involved with the incident. If there are several parties, the information disclosed to each party is strictly limited to information concerning the party in question.

When the incident has been reported forwards or has been handled in some other way, the sender receives an acknowledgement of the report having been handled.

If Funet CERT receives a response or a report regarding the situation from other party, the information is also forwarded to the initial reporter.

Coordinating at Funet CERT

If the incident concerns several parties, Funet CERT can act as the coordinator for information echange.

If the incident concerns only one or two Funet member organizations, we can act as the coordinator or the parties can exchange messages directly. However, we would like to be informed of the incident details.

Why should incidents be informed to Funet CERT

It is a good policy to inform Funet CERT of IT security incidents because

- The best way to prevent attacks is a joint response to them
- An organization's IT security instructions require that a report be filed
- Filing a report helps to prevent an attack or other nuisance
- You need additional information or technical guidance
- Collaboration is necessary to get an idea of the whole scenario
- The incident may be a part of a more extensive entity
- By filing a report you can improve awareness on IT security issues