Incident Report Template DRAFT

The following template may be used to report a security incident affecting eduGAIN to the eduGAIN CSIRT.

How to report a security incident

Please follow the eduGAIN Security Incident Handling Procedure to report a security incident to abuse at edugain.org (eduGAIN CSIRT PGP key https://edugain.org/edugain-security). You will find it useful to print the eduGAIN secproc.pdf (THIS NEEDS TO BE CREATED 😊).

FROM: <you>
TO: abuse@edugain.org
SUBJECT: [TLP:AMBER] Security incident suspected at <site>
** AMBER Information - Limited Distribution **
** This may be shared with trusted security teams on a need-to-know basis **
** see https://www.first.org/tlp/ for distribution restrictions **

Dear eduGAIN CSIRT,

A suspected security incident has been detected at <ENTITIES_NAME>.

Summary of the information available so far:
<Ex: A malicious SSH connection was detected from 012.012.012.012. The extent of the incident is unclear for now, and more information will be published in the coming hours as forensics are progressing at our site. However, all sites should check for successful SSH connection from 012.012.012.012 as a precautionary measure.>

Follow-up message

This template can be used to provide a detailed view of the incident, and may be completed and resent as the investigation progresses. The data in this email will, in most cases, be forwarded to all security contacts, but some filtering might be applied if deemed necessary.

FROM: <you>
TO: abuse@edugain.org
SUBJECT: [TLP:AMBER] Security incident suspected at <ENTITY_NAME>
** AMBER Information - Limited Distribution **
** This may be shared with trusted security teams on a need-to-know basis **
** see https://www.first.org/tlp/ for distribution restrictions **

Dear EGI CSIRT,

A security incident has been detected at <ENTITY_NAME>.

- Short summary of the incident
<Provide a high-level overview of the incident>

- Systems affected
<List of compromised systems and/or systems running suspicious user code.>
ex: idp.mysite.org (123.123.123.123)>

- The attacker used the following systems to connect to the affected systems:
<The remote host from where the attacker is likely to have connected from.>
ex: 123.adsl.somecorp.com (012.012.012.012)>

- Evidence of the compromise, including timestamps (ex: suspicious files or log entry)
<Ex: the attacker logged in has root from 123.adsl.somecorp.com (012.012.012.012)>

Times are UTC:
2025 Mar 24 12:00:09 grid-ui-101 sshd[13896]: Accepted password for root from 012.012.012.012>

- What was lost, details of the attack
<Provide available details on the extent of the compromise.>
Ex: System logs revealed the attacker guessed the root password of idp.mysite.org (123.123.123.123)
System log shows on 2025 Mar 24 12:00:09 (UTC) hundreds of failed attempts to login as root, then, suddenly the attacker successfully logged in [...] etc. The attacker created the identities ABC and XYZ, placed a trojan and possibly compromised the credentials of users: DEF, UVW>

- If available and relevant, the list of other eduGAIN participants possibly affected
<Ex: Suspicious new identities ABC and XYZ where created:

- Possible vulnerabilities exploited by the attacker
<Ex: the attacker exploited a weak root password and gained further access by exploiting CVE-2009-1234 against [...] etc.>

- Actions taken to resolve the incident <Ex: Disk images have been saved, systems have been reinstalled from scratch with new, strong root passwords, and SSH has been configured to prevent "root" logins with password.>

- Recommendations for other sites, actions suggested
<Ex: Sites should check and report any successful SSH connection from 123.ads1.somecorp.com between Mar 24 12:00:09 (UTC) and Mar 24 17:00:00 (UTC). It is also recommended to avoid direct SSH access, and to configure sshd with "PermitRootLogin without-password".

Service Providers should check for activities related to identities ABC,XYZ>

- Timeline of the incident
<Ex:
2025-03-24 09:12:43 UTC Multiple SSH connection attempts from 12.012.012.012 2009-03-24 12:00:09 UTC Attacker connects as root on idp.mysite.org (123.123.123.123) from 012.012.012.012
2025-03-24 13:01:03 UTC creation of identity XYZ
2025-03-24 15:00:00 UTC Site security team investigating
2025-03-24 15:34:00 UTC EGI security contacts informed [...]>

>