Keeping EGI secure

EGI CSIRT: Prevention - Response - Training

Keeping EGI secure

EGI CSIRT: Prevention - Response - Training

EGI is a federated e-Infrastructure set up to provide advanced computing, storage and data services for research and innovation.

The EGI e-Infrastructure is publicly-funded and comprises almost 300 data centres and cloud providers spread across Europe and worldwide.

www.egi.eu

Meet the EGI CSIRT

Computer Security and Incident Response Team

The EGI CSIRT builds on networks of experts.

The team is made up of security officers and experts distributed over several countries and based at national e-Infrastructures (often abbreviated as NGIs) and one European research organisation (CERN). They work together to keep the e-Infrastructure safe, making sure that disreputable types don't find a red carpet on the way in.

The EGI CSIRT is led and coordinated by the EGI Security Officer, whose role and mission is defined by the security policies approved by the EGI Federation.

The team provides operational security for the EGI infrastructure.

The EGI CSIRT looks after the EGI Federation of data centres as well as its infrastructure components and users. Following key principles of EGI, the data centres are bound by the policies and procedures of the EGI security framework, while retaining operational autonomy.

A large part of the EGI CSIRT work is to ensure that the procedures are followed and that every data centre knows what to do and when.

EGI CSIRT is certified by Trusted Introducer since October 2014.

Trusted Introducer is a community of about 300 CSIRT teams from large scale organisations classified according to three levels: listed, accredited and certified. The EGI CSIRT was the 5th team to achieve the top certified status.

This means that the entire EGI CSIRT, its procedures, policies & operations were positively evaluated after an external peer review.

Activities

What do we do?

EGI CSIRT activities cover:
> **prevention of security incidents** (security monitoring, vulnerability handling, risk assessment and mitigation),
> **incident response** (digital forensics and mitigation) and
> **security training.**

The team relies on the security staff at the EGI federated data centres, national e-Infrastructures and CERN to keep EGI secure for the benefit of its users.

EGI CSIRT ensures effective security coordination within the EGI Federation and liaises with other e-Infrastructures (e.g. EUDAT, PRACE, XSEDE) and the National Research and Education Networks (NRENs).

Activity groups

Day-to-day security operations are handled by the **Incident Response Task Force** - a small team of about half a dozen security officers working across countries and organisations. These are the guys & the gals on watch who pick up the phone and act as first responders to reports of security incidents within EGI. They are volunteers working in shifts and you will find one on duty 24/7, holidays included.

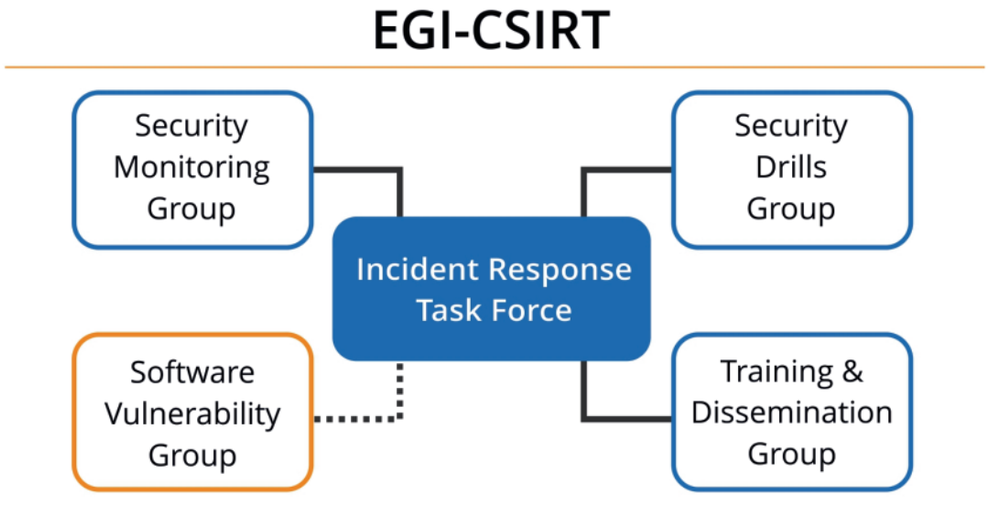
The **Security Monitoring Group** maintains a monitoring framework that collects and evaluates data from all EGI federated data centres. This framework enables the EGI CSIRT to check basic security characteristics of services, including software patching levels and deployed mitigations.

The **Security Drills Group** tests the incident response capabilities of the EGI federated data centres and improves collaboration among the distributed teams. Because you can never get too comfortable, the group organises drills where a red team "attacks" the infrastructure while the blue team "defends" it using and testing incident response tools and existing procedures.

The **Training and Dissemination Group** collects best practices and organises different types of events to train security staff across the EGI Federation.

The **EGI Software Vulnerability Group** works closely with the EGI CSIRT to minimise risks to the e-infrastructure arising from software vulnerabilities.

This group investigates potential and existing software vulnerabilities, their relevance to EGI and assesses the risk to the EGI infrastructure. When appropriate, the group issues advisories to the EGI federated data centres.



Prevention

Keeping the bad guys out

The larger part of the work of the EGI CSIRT is to prevent security incidents. The EGI Software Vulnerability Group assists in this aim, by handling vulnerabilities reported in the software used in the infrastructure.

Software vulnerabilities may be reported by anyone. Vulnerabilities in operating systems are often announced by the technology distributors and flagged by system administrators across the federation. Vulnerabilities in software produced by collaborating projects and institutes are likely to be reported by developers, group members and other security experts in EGI.

After a vulnerability is found, the group investigates if it has potential to become a problem to the EGI infrastructure and, if yes, what is the risk involved. During risk assessment, the vulnerability is placed the in one of the categories: 'Critical', 'High', 'Moderate' or 'Low'.

If deemed necessary, the Software Vulnerability Group will issue an advisory with recommended actions for data centres to fix the problem before someone decides to exploit the vulnerability for selfish interest.

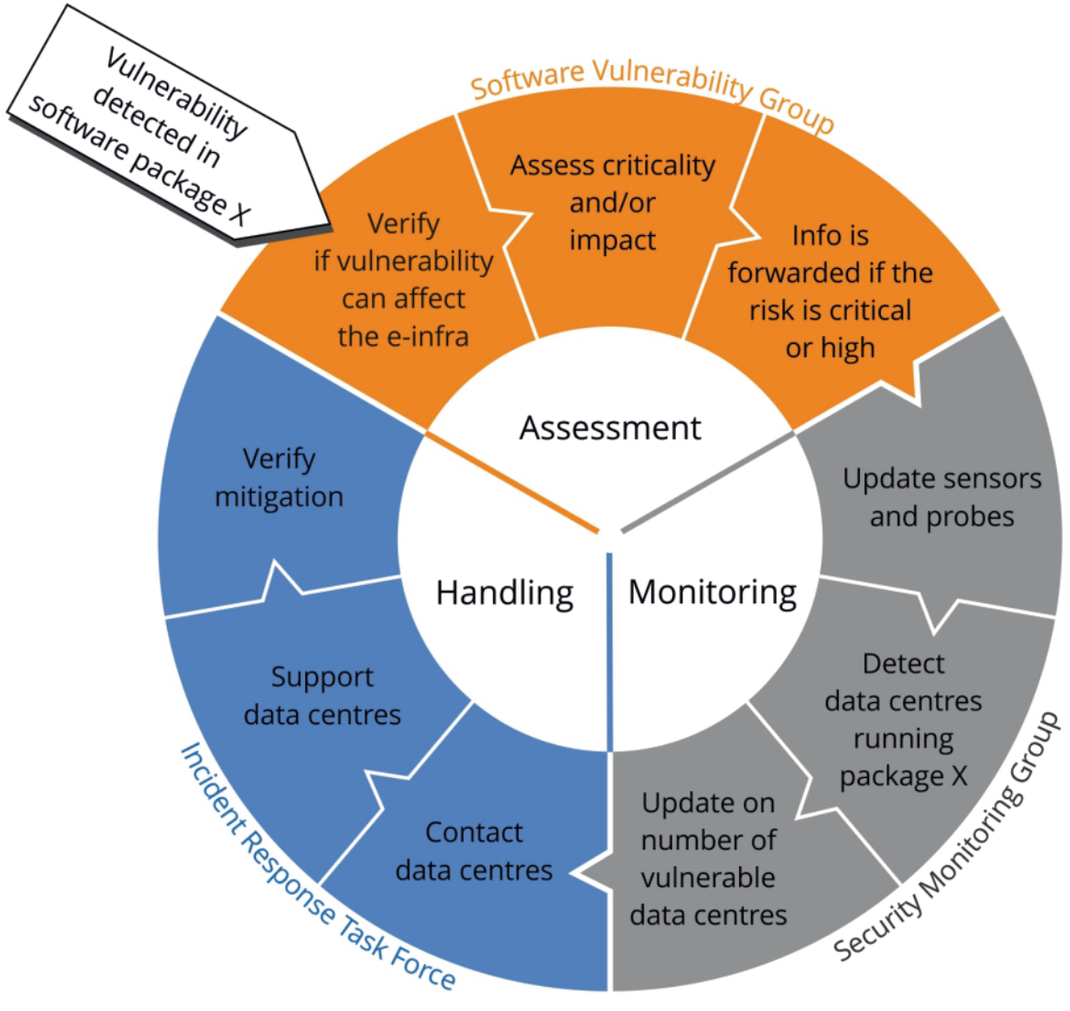
Vulnerabilities can also be detected by monitoring. The EGI CSIRT deploys a framework to monitor software vulnerabilities with potential to affect the infrastructure. The monitoring framework collects information about packages installed on compute nodes available to users and detects missing software updates.

Once a Critical vulnerability is detected by the monitoring, the EGI CSIRT contacts the centre asking for an action, usually to apply the requested updates. Given the large number of sites and machine, the EGI CSIRT quite often fight regressions of vulnerabilities that show up repeatedly.

Thank you!

The EGI CSIRT thanks the good souls who found and reported vulnerabilities to us.

It's appreciated!

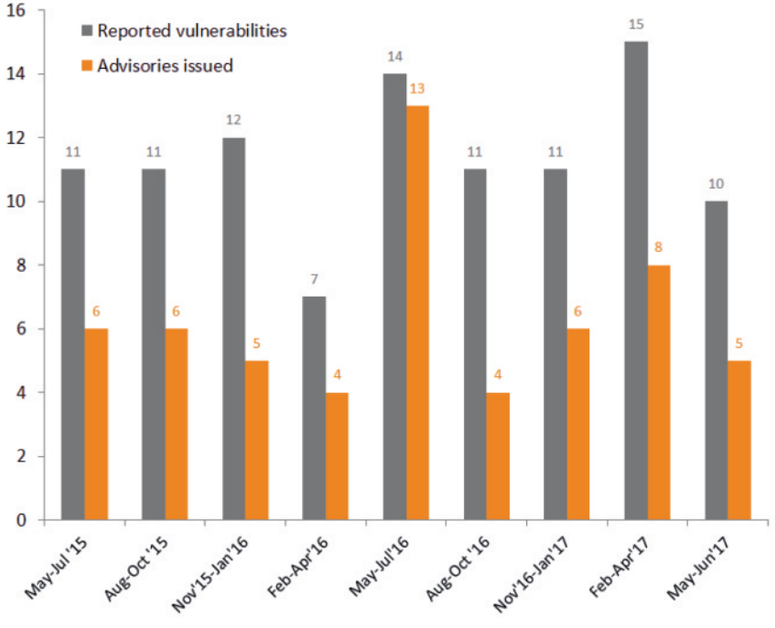


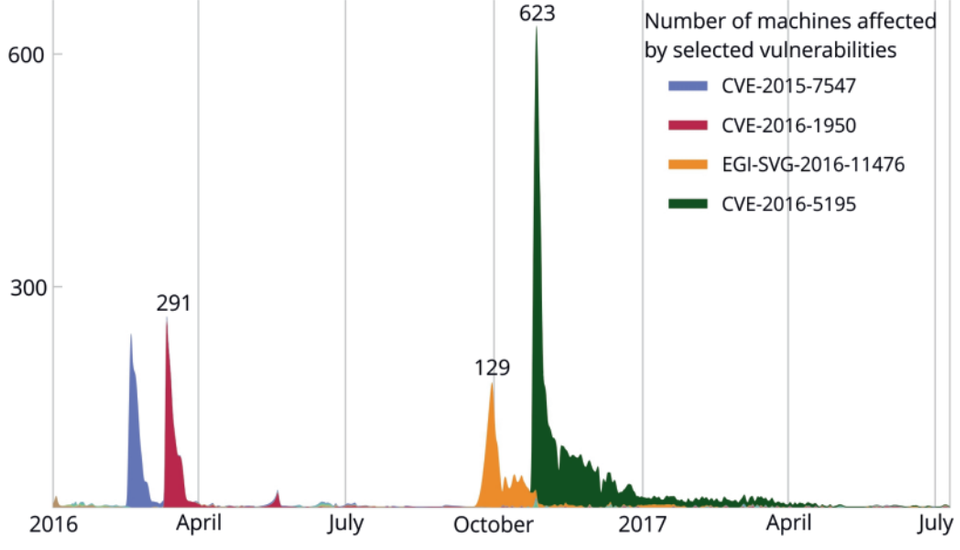
If you find a vulnerability

Please report it to the Software Vulnerability Group: **report-vulnerability@egi.eu**.

Please *do not discuss* the vulnerability in open forums or blogs, as this may compromise our mitigation strategies.

Vulnerabilities in numbers





More information:
Some vulnerabilities are straightforward and can be handled very quickly, some need special treatment. For instance, CVE-2016-5195 is a severe vulnerability in the Linux Kernel. Fixes were not easy to provide nor apply and many data centres opted to apply a mitigating configuration and, therefore, getting rid of the vulnerability completely took a longer time.
TL;DR: even several hundreds of vulnerable data centres can be fixed within two weeks.

Response

When rainbows hit the fan

Security incidents often happen when someone exploits a vulnerability to gain unauthorised access to the computing infrastructure. Intrusions are usually detected by the EGI data centres and reported to the EGI CSIRT who then coordinates the investigation and response.

The work starts with looking for clues and leads, just like what we see at the beginning of crime-oriented television episodes. Crime scene investigators use forensic evidence to understand what happened. EGI CSIRT prefers logs and files to fingerprints and exotic fibres, but the goals are similar.

Digital forensics is about investigating evidence and leads to understand who the culprits are, what they are after, how they got access to the system, and how their malware works.

Analysing malware helps to understand a particular attack but it can also provide remote scanning tools, Indicators of Compromise and, potentially, internet addresses of infected systems that will help the community to react to the threat and, if possible, track the malicious intruder.

Security incidents often span multiple organisations and country borders. EGI CSIRT relies on established links and trusted relationships with the community to collect and evaluate all the available information about an incident. Good communication lines between EGI CSIRT and the data centres is the secret weapon against large-scale incidents.

Number of incidents since 2010

All incidents were successfully and quickly contained, thanks to the security coordination that EGI CSIRT provides across the federation.

Case Study: VENOM rootkit

The VENOM rootkit was a malware designed to maintain unrestricted and permanent access to compromised Linux systems.

The attackers, having obtained root access through other means, were able to deploy a malicious kernel module and a userland binary, and configure them to be loaded upon the boot of the machine. This malware provided several features such as execution of an interactive shell or manipulating files on the compromised system.

When the VENOM rootkit was detected in a server at an EGI data centre in December 2016, the EGI CSIRT moved into the digital crime scene. By reverse engineering the malware, they were able to understand how the malware operated and, more importantly, what was its backdoor mechanism. This allowed the team to test suspicious systems and provide guidance how to check if the rootkit was installed.

This analysis lead to the discovery of an additional 25 servers outside the EGI Federation where VENOM was active but not yet detected.

Training

Practice makes perfect

Keeping the EGI infrastructure secure requires an understanding of attack and defence techniques that goes beyond the average skillset of system administrators.

Security training is vital to guarantee that local teams are able to use available information for a complete incident response.

Plugging the knowledge gaps is part of the EGI CSIRT mission and over the years the team has worked to get the EGI community ready for action. The EGI CSIRT has a diverse catalogue of training modules, developed by or the team or by partner institutions.

EGI CSIRT training sessions

Defensive training unleashes an incident in a controlled environment to test and improve defence skills. Based on actual attacks, the training is intended to look as realistic as possible to prepare the teams for real life attacks and familiarise them with response procedures.

Offensive training turns the world upside down and asks the security teams to go on the attack. The teams learn about attacking tools, how to spot weak points and how to disguise one's tracks. By thinking as an attacker, they will know better what to expect during incidents. The training module was provided by Masaryk University and its CSIRT team.

Digital forensics training is all about finding clues to understand what happened. The teams look into the logs and the files of a compromised system and learn how to spot the origin of the attack and what were the weak points explored by the attackers.

Roleplay training brings it all together. The participants are divided into teams and enact an incident inspired by real life. The teams play all incident-response roles, from site admins to managers, to learn that incident response is not only about technical know-how but also how it relies on effective communications.

Training events		attendants
Defensive	Best practices for managing system security on Linux systems (ISGC 2015) *	18
Defensive	Security training for Cloud Providers, VM admins, maintainers (EGI Community Forum 2015) *	15
Defensive	Incident response and federated identity management (ISGC 2016)	15
Forensics	Penetration testing hands-on training (UK HEP SYSMAN)	20
Forensics	Security incident detection, analysis and handling in the world of Federated Cloud services and distributed computing infrastructures (ISGC 2017)	18
Offensive	Security session, Offensive Training (France Grilles Annual Meeting 2016) **	12
Offensive	Security Training (EGI Conference 2015) **	30
Defensive	Best practices for managing system security on Linux systems in Grids and Clouds (ISGC 2015)	18
Roleplay	Federated AAI meets reality, Security Incident Handling Role Play (Trusted Introducer meeting 2016)	15
Roleplay	Federated AAI meets reality, Security Incident Handling Role Play (DI4R 2016)	25

* with Nixon Security; ** with Masaryk University

Future challenges

No rest for the wicked

Federated Cloud Security

EGI will continue to develop its cloud services portfolio in the coming years and Federated Cloud security will have to evolve accordingly.

The EGI Federated Cloud is a challenging environment because it's not very forgiving for the users. We cannot expect researchers to be system experts, we cannot count on them being aware of all the risks, vulnerabilities and procedures, and we cannot blame them for this.

The challenge will be to make the Federated Cloud securely user-proof. It will be a major effort of operations management but there is precedent in commercial companies and the technology is available.

Compromised federated identities

As Authentication and Authorisation methods for large user communities move towards federated access models, how do we handle individual problem users?

While this evolution is welcome, we have to make sure that we are still able to do the basic steps in incident response, for example suspending a compromised account.

The challenge will be to retain the capacity of responding to incidents promptly in an increasingly complex landscape where more and more identity providers are involved.

Widening collaborations

The next few years will see EGI widening its collaboration and integration with EUDAT and other e-Infrastructures. This will bring huge benefits for the researchers who currently rely on separate service catalogues for their work.

The challenge will be to work closely with other security teams to harmonise operational security policies and procedures into a coherent set.

Contacts

Website:
https://csirt.egi.eu

EGI Security Officer:
Sven Gabriel (NIKHEF)

To report a vulnerability:
report-vulnerability@egi.eu
(please don't discuss it in open forums)

To report an incident:
> *EGI data centres* : follow https://wiki.egi.eu/wiki/SEC01
> *Everyone else* : abuse@egi.eu

Acknowledgements

This publication was prepared by the EGI CSIRT and the Communications Team of the EGI Foundation.

The EGI CSIRT is a coordination service of the EGI Federation funded by the EGI Council and contributions of the institutions represented in the team.

The EGI-Engage project is co-funded by the European Union (EU) Horizon 2020 program under grant 654142.

The content of this publication is correct to the best of our knowledge as of July 2017.

www.egi.eu