EGI-CSIRT Operational Security

Sven Gabriel

Operations Update

EGI-Engage is co-funded by the Horizon 2020 Framework Programme of the European Union under grant number 654142

Critical Vulnerabilities

Apache Struts vulnerability

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638
- The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 mishandles file upload, which allows remote attackers to execute arbitrary commands via

  ...

  crafted Content-Type HTTP header, as exploited in the wild in March 2017.
- This is used in voms.
- A lot media interest.

Apache Struts Timeline

- 10.Mar CSIRT got aware of the vulnerabiity (Vincent, Fyodor), Reported to SVG
- first assessment: we may not be affected by CVE-2017-5638, we use an too old version, but . . .
- A lot more Crtitical vulnerabilities related to CVE-2017-5638 got back on the radar (CVE-2011-3923, CVE-2012-0391, . . .)
- 15. Mar Vincenzo/Mischa found we are affected, successfully exploited remote code execution vulnerability:**CRITICAL**
- VOMS team immediately started to work on patches.
- Mitigation is to block port 8443 on voms-admin (Nikhef implemented this on the test system).
- Other IRTF Memebers reported to have applied the same mitigation.

Apache Struts Timeline II

- 17. Mar. Advisory Draft available
- 17. Mar. mitigation rpm available (limit access authn with igtf certificates)
- 20. Mar discussion in IRTF Telco
- 20. Mar targeted comm. to sites having a voms server registered in gocdb by IRTF
- 23. Mar VOMS Admin 3.6.0 is now on the VOMS repository.GGUS ticket for inclusion in UMD:
- 27-03-17 09:57 (Broadcast) Advisory sent by SVG
- IRTF monitors the situation at voms servers

Incidents

EGI-20170322-01: IISAS-FedCloud

- 22. Mar Report received
- malicious SSH connection was detected from 124. . .
- BitCoin Mining
- Attack Vector: One openstack site miss-configured (VNC exposed to the world) and exploited remotely.
- Openstack documentation not clear on the configuration (accessability of VNC services)
- Vulnerable settings confirmed by CERN

EGI-20170322-01: Impact on our Infra

- Depends how other sites are configured:
- If management network or VNC is properly protected: None
- If management network or VNC is exposed internally but not externally (like CERN): Medium/high
- If exposed to the world (like IISAS-FedCloud): Critical
- 23 Mar Broadcast with recommendations sent.