Compute Node scanning tool

Jeny Teheran, Fermilab

Thematic CERN school of computing

Split, Croatia 2022

Context

OSG: 20+ contributors in the US, South and Central America

Open Science Grid

OSPool

The Open Science Pool (OSPool) aggregates mostly opportunistic computing resources from contributing clusters at campuses and other organizations, making them available to the US-based open science community.

US CMS Operations Program

https://osg-htc.org/services/open_science_pool.html

OSG-SEC-2022-03-31 CRITICAL Expat XML parser arbitrary code execution vu

OSG-SEC-2022-03-31 CRITICAL Expat XML parser arbitrary code execution vulnerability

Dear OSG Security Contacts,

Vulnerabilities have been found concerning the expat XML parser, including two which may lead to arbitra
parser is a library, written in C, which is a dependency for various other software, including VOMS server a

IMPACTED VERSIONS:

xmltok_impl.c in Expat (aka libexpat) before 2.4.5

WHAT ARE THE VULNERABILITIES:

xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for w
context. xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator cha

Of principal concern are VOMS client and server packages, as well as HTCondor which also utilizes the VO

WHAT YOU SHOULD DO:

Sites running software which is dependent on expat should update urgently, including those running a VC
updated service [4][5][6].

REFERENCES

[1] https://access.redhat.com/errata/RHSA-2022:1069
[2] https://access.redhat.com/security/cve/cve-2022-25235
[3] https://access.redhat.com/security/cve/cve-2022-25235
[4] http://mirror.centos.org/centos/7/updates/x86_64/Packages/
[5] https://security-tracker.debian.org/tracker/CVE-2022-25235
[6] https://people.canonical.com/~ubuntu-security/cve/2022/CVE-2022-25235

Please contact the OSG security team at security@opensciencegrid.org if you have any questions or conce

OSG Security Team

WHAT AND WHY?

WHAT TO DO?

HOW URGENT?

Does that mean our sites patch according to urgency?

No ☹

Understanding why:

- The absence of a security policy enforcement mechanism for volunteered resources:
  - Aggregated resources operate under an integrated security framework based on trust.
  - Threatening site suspension for not following mitigation or resolution action will be detrimental to the volunteer nature of the OSPool.
- Sometimes, upgrades break services and dependencies (EOL, unsupported.
  - Particularly painful for VOs and experiments actively taking data.
- But, our vulnerability handling procedures have deeper issues…

Vulnerability handling at OSG and US CMS

- OSG security team has little visibility into the packages (*and vulnerabilities*) deployed at compute nodes.
- Security advisories and announcements range from Linux kernel vulns, grid software technologies, open-source software libraries, to CISA security advisories.

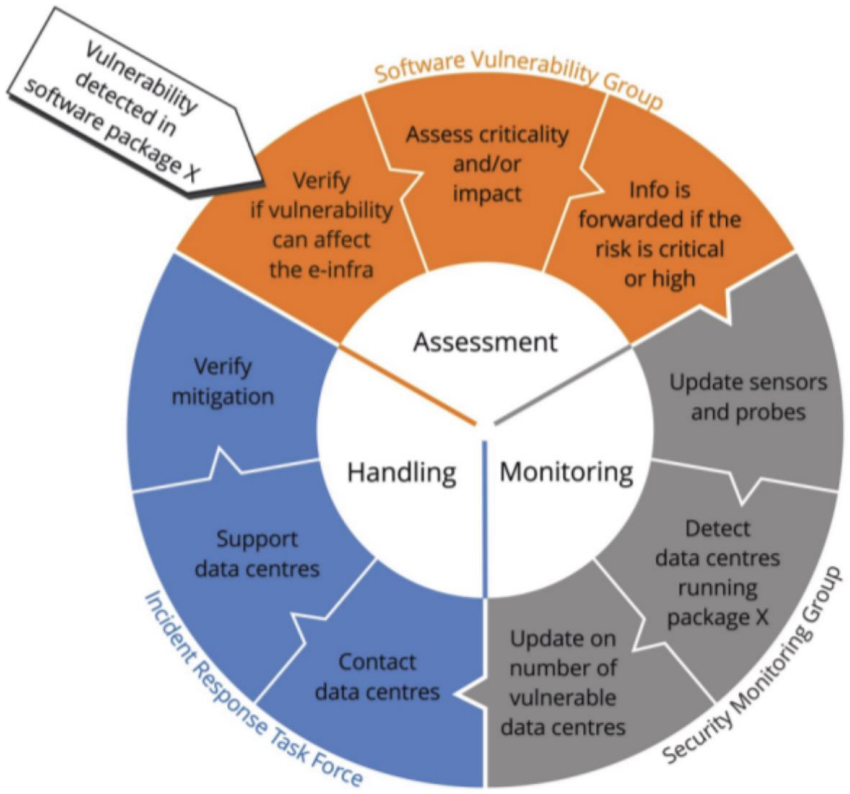
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

- Site admins with reduced patching capabilities:
  - Sometimes, our mitigation or resolution action conflicts with campus cybersecurity teams perceived risk-level.
  - Urgency also in conflict with patching and maintenance schedules.

Vulnerability handling, continuous process

https://csirt.egi.eu/activities/:

Root Cause of our issues



Little visibility into the packages deployed at compute nodes:

- Heterogeneous resources and software environments
- Requires individually checking with sites and contributors if they are running software package X?

What about Pakiti?

We tried a similar tool a few years ago:

- Requires active monitoring and technical support
- Joining the OSPool requires minimal software installation at sites

Borrowed from Sven Gabriel S18,
https://indico.cern.ch/event/1106023/contributions/4915298/attachments/2462974/4222999/Vulnerability_management_v1.pdf

What to do?

- A tool to monitor and assess potential risk in the Open Science pool will allow the security team to make informed decisions about handling vulnerability announcements and accurately estimate exposure to various risks.
- 1st goal: Build and maintain an information asset inventory tool:
  - Customizable payloads
  - Avoid running multiple times on the same host or at least avoid duplicating results
  - Securely report results back to be aggregated
  - No special configuration required, installation or software packages or special privileges

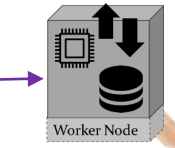
Compute Node scanning tool

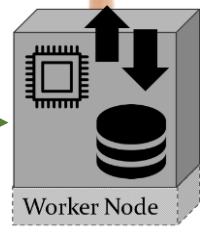
Job 1

Job 2

Queries UI

Web Service
(Aggregation &
Analysis)





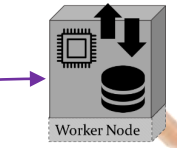

```
{
“id”:”000001”,
“reporting-site:”site”,
“kernel”:”5.4.143-1.fc25.qubes.x86_64”,
”packages”:[“package 1”,”package 2”,”package 3”],
“patches”:[“available patch 1”,”available patch 2”,”available patch 3”]
}
```

Compute Node scanning tool

1. Campaign mode
2. Targeted sites

Job 1

Job 2



Queries UI

Web Service (Aggregation & Analysis)

Information also valuable to attackers

```
{
“id”:”000001”,
“reporting-site:”site”,
“kernel”:”5.4.143-1.fc25.qubes.x86_64”,
”packages”:[“package 1”,”package 2”,”package 3”],
“patches”:[“available patch 1”]
}
```

In summary

- An information asset inventory, identify vulnerable systems, and gather other information about our volunteer infrastructure.
  - Note that some of these capabilities already exist and may not require additional development to implement.
- Expand the tool: monitoring for vulnerability patching across OSPool contributors.
- 2nd idea: monitor dependencies between OS libraries, grid software.