ESGF Scanner

8^{th} ESGF F2F, Washington DC. Dec 2018

Prashanth Dwarakanath

LIU/NSC

Dec 06 2018

The Need

- ESGF Security incident: vulnerabilities had been around for a long time.
- a clear need for regular checking of components against known vulnerabilities.
- a need for a system that would not only serve alerts, but also need alerts to be 'acknowledged' or discarded.
- Scanning/checking time would have to be low, to allow for multiple checks each day.

What is ESGF Scanner/CVEChecker?

- **CVEChecker** is a tool for aggregating CVE information from multiple sources, and managing a local vulnerability (CVE) database.
- makes it easy to process the information that is already available.
  - coded in Python 3.
  - uses feeds from NVD and Redhat.
  - can be kept updated using a cron job.
  - development supported by the Swedish National Infrastructure for Computing (SNIC).
  - https://github.com/snic-nsc/cvechecker
- **ESGF Scanner** is a wrapper-package for using **CVEChecker** to check for vulnerabilities against ESGF components.
  - scripts used to retrieve package lists (jar lists, python packages) from an ESGF node.
  - writes out manifest, generates configuration file for **CVEChecker**.
  - invokes **CVEChecker** with the ESGF specific configuration.
  - development supported by the Copernicus project.
  - https://github.com/snic-nsc/esgf_scanner

Design-considerations

- Information is more useful if actionable, like an alert.
- CVE information evolves during its life; initial details are little, and more details get added as more is learned.
- Need to get alerts as soon as it is deemed relevant.
- Keyword-based search on descriptions, product descriptions in affected product lists, CPEs etc provide multiple ways to find relevant hits.
- Combining search filters increases chances of getting alerts earlier.

ESGF Scanner scripts

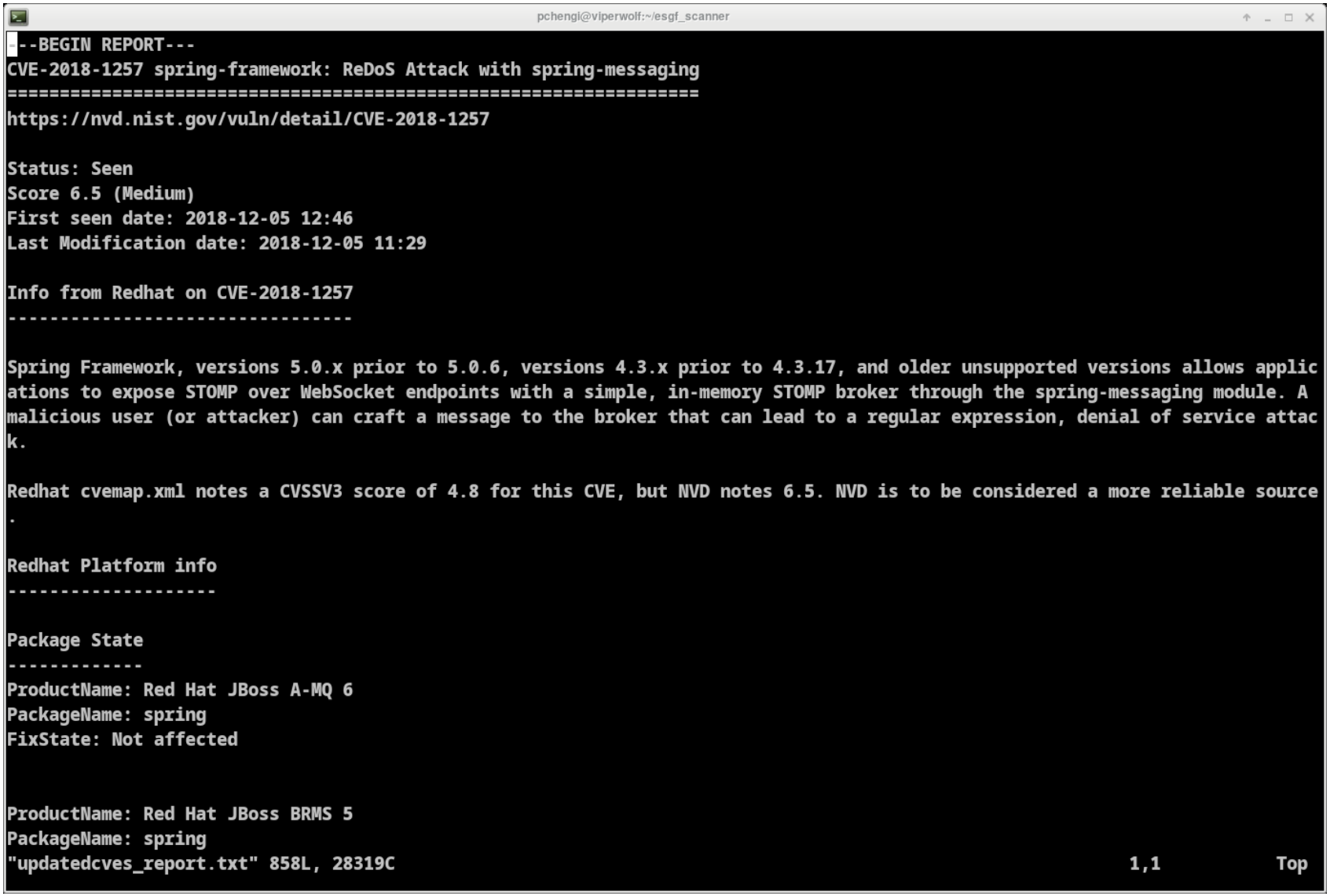
- ESGF specific abstraction to use **CVEChecker**.
- `rungetpackagelists.sh` fetches package lists from ESGF node which can be sshed to, as root or root-equivalent user.
- prepares package manifest.
- creates `esgf.conf`, an input-file for **CVEChecker**, based on the packages found.
- Additional packages can be specified by hand.
- `run_workflow.sh` generates a configuration file and performs a **CVEChecker** run.
- `runesgfscanner.sh` does the same, but is meant to email reports to configured recipients.

Output

pchengi@viperwolf:~/esgf_scanner

```
[pchengi@viperwolf esgf_scanner]$ time (bash run_workflow.sh )
We are asking to mute the following CVEs which seem to have been updated
CVE-2018-1257,CVE-2018-1259,CVE-2018-1336,CVE-2018-8014,CVE-2018-8039
We have new CVE hits against our packages.
CVE-2018-1000643

real    2m22.769s
user    0m48.228s
sys     0m5.323s
[pchengi@viperwolf esgf_scanner]$ bash cvechecker/matchstats.sh esgfreport.txt
Total number of matching CVEs: 16
antisamy:1
cxf:1
log4j:1
mysql-connector-java:1
spring:1
Spring Framework:1
Apache Tomcat:2
django:2
hadoop:2
jetty:4
[pchengi@viperwolf esgf_scanner]$
```

Output

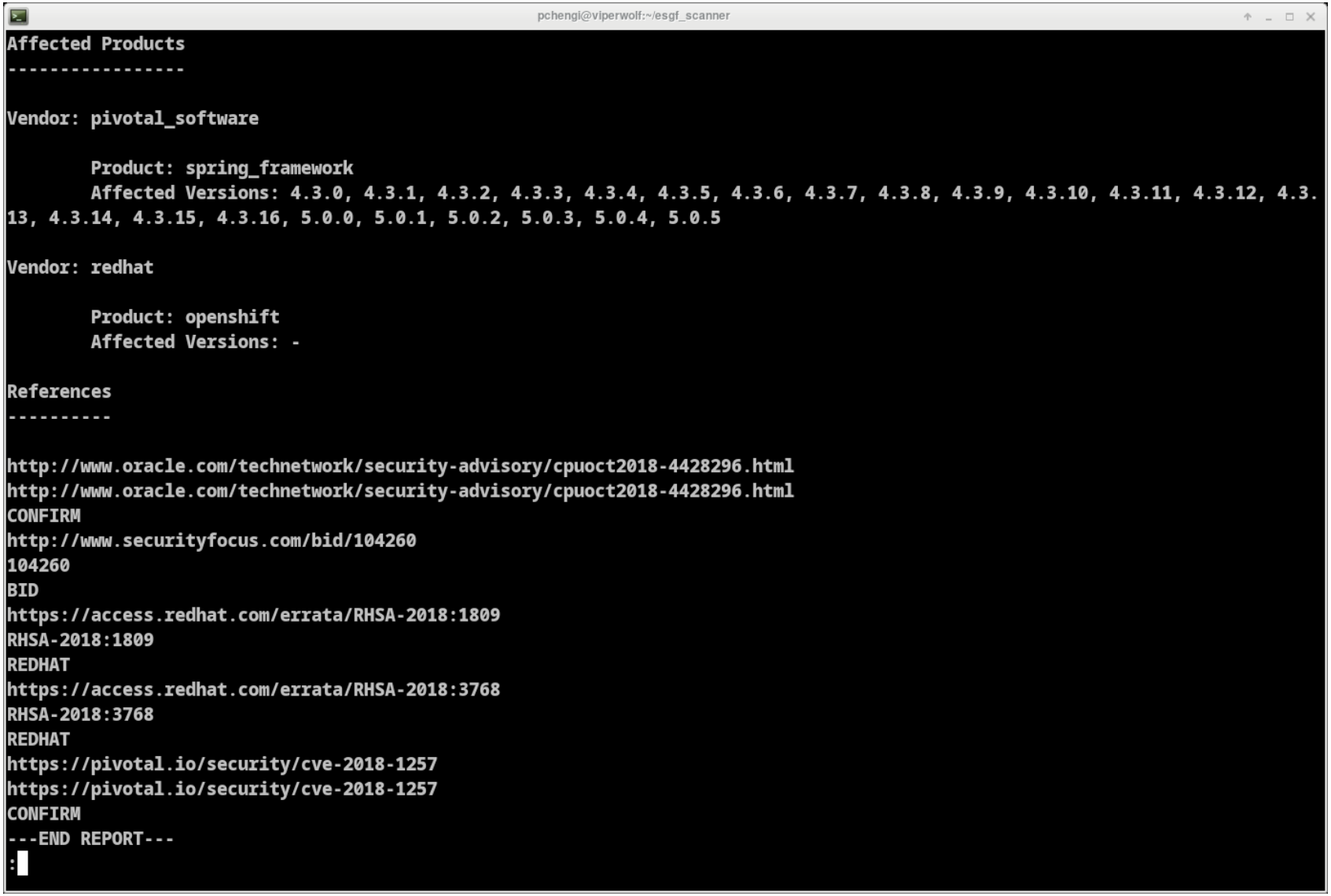

pchengi@viperwolf:~/esgf_scanner
---BEGIN REPORT---
CVE-2018-1257 spring-framework: ReDoS Attack with spring-messaging
https://nvd.nist.gov/vuln/detail/CVE-2018-1257
Status: Seen
Score 6.5 (Medium)
First seen date: 2018-12-05 12:46
Last Modification date: 2018-12-05 11:29
Info from Redhat on CVE-2018-1257
Spring Framework, versions 5.0.x prior to 5.0.6, versions 4.3.x prior to 4.3.17, and older unsupported versions allows applic
ations to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A
malicious user (or attacker) can craft a message to the broker that can lead to a regular expression, denial of service attac
k.
Redhat cvemap.xml notes a CVSSV3 score of 4.8 for this CVE, but NVD notes 6.5. NVD is to be considered a more reliable source
.
Redhat Platform info
Package State
ProductName: Red Hat JBoss A-MQ 6
PackageName: spring
FixState: Not affected
ProductName: Red Hat JBoss BRMS 5
PackageName: spring
"updatedcves_report.txt" 858L, 28319C
1,1
Top

Output

pchengi@viperwolf:~/esgf_scanner

```
Affected Package Info
---------------------
ProductName: Red Hat JBoss Fuse 7
ReleaseDate: 2018-12-04T00:00:00
advisory_url: https://access.redhat.com/errata/RHSA-2018:3768


ProductName: Red Hat OpenShift Application Runtimes 1.0
ReleaseDate: 2018-06-07T00:00:00
advisory_url: https://access.redhat.com/errata/RHSA-2018:1809



Info from NVD on CVE-2018-1257
------------------------------
Spring Framework, versions 5.0.x prior to 5.0.6, versions 4.3.x prior to 4.3.17, and older unsupported versions allows applic
ations to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A
malicious user (or attacker) can craft a message to the broker that can lead to a regular expression, denial of service attac
k.

Affected Products
-----------------

Vendor: pivotal_software

        Product: spring_framework
        Affected Versions: 4.3.0, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.5, 4.3.6, 4.3.7, 4.3.8, 4.3.9, 4.3.10, 4.3.11, 4.3.12, 4.3.
13, 4.3.14, 4.3.15, 4.3.16, 5.0.0, 5.0.1, 5.0.2, 5.0.3, 5.0.4, 5.0.5

Vendor: redhat

        Product: openshift
        Affected Versions: -
:
```

Output


pchengi@viperwolf:~/esgf_scanner
Affected Products

Vendor: pivotal_software
Product: spring_framework
Affected Versions: 4.3.0, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.5, 4.3.6, 4.3.7, 4.3.8, 4.3.9, 4.3.10, 4.3.11, 4.3.12, 4.3.13, 4.3.14, 4.3.15, 4.3.16, 5.0.0, 5.0.1, 5.0.2, 5.0.3, 5.0.4, 5.0.5
Vendor: redhat
Product: openshift
Affected Versions: -
References
----
http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
CONFIRM
http://www.securityfocus.com/bid/104260
104260
BID
https://access.redhat.com/errata/RHSA-2018:1809
RHSA-2018:1809
REDHAT
https://access.redhat.com/errata/RHSA-2018:3768
RHSA-2018:3768
REDHAT
https://pivotal.io/security/cve-2018-1257
https://pivotal.io/security/cve-2018-1257
CONFIRM
---END REPORT---
:

Limitations/Caveats

- CVEs evolve over time; very little info initially, but gets more detail over time.
- It could be days or even weeks after a CVE becomes public, before the affected product information is updated.
- A keyword-based hit could raise an alert much sooner.
- False-positives; need to spend time to mute unrelated issues.
- Time also needed to study matches, CVE descriptions, and add additional keywords to increase hit ratio.

Status

- ESGF Scanner has now been integrated with the Jenkins setup at LLNL.
- ESGF Scanner can be run at the end of a successful installation of ESGF, to generate a manifest file and scan report.
- Feedback and help are very welcome!