STAMVS
NETWORKS

Detection of CVE-2022-22963/5 (Spring4Shell) using Stamus Security Platform (ND/NDR/PM)

On March 31, 2022, VMware published a Common Vulnerabilities and Exposure (CVE) alert identifying a vulnerability in the Spring Java Framework and Spring Cloud Function which can result in remote code execution (RCE). Those critical alerts are:

CVE-2022-22693 - applies to Spring Cloud Function version <=3.1.6 and <= 3.2.2
CVE-2022-22965 - applies to Spring Framework <=5.3.17 and <=5.2.19

We recommend you patch any vulnerable systems as soon as possible.

In the meantime, you may take the following steps to help determine if any of your systems have been attacked in the past, are currently under attack or vulnerable.

DETECTION AND ESCALATION

Please follow the steps listed below in the Stamus Security Platform at the Stamus ND/NDR license tiers (formerly Scirius Security Platform), "Hunt" interface.

Create a Filter

NOTE: Portions of this are not applicable to the Stamus Probe Management license tier

Any CVE number can be searched in the Hunt interface.

To create a filter:

1. In Hunt, click on the magnifying icon next to any signature (first group Signatures on the Dashboard tab).

2. Click on the pencil/Edit icon on the resulting filter displayed as "Active Filters:".
3. Type the CVE number or a text descriptor with a wildcard (*) it at each end (for example: *CVE-2022-22965* or *Spring4Shell*)
4. Select the checkbox "Wildcard view"
5. Click Save
6. You are now ready to review the results and events in the Dashboard, Host Insights and Alert views

The example screenshot below shows how to do that for "CVE-2022-22965"
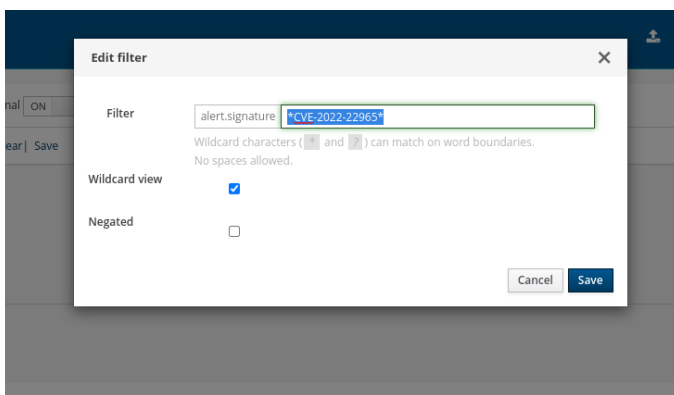
The example screenshot below shows how to do that for "Spring4Shell"
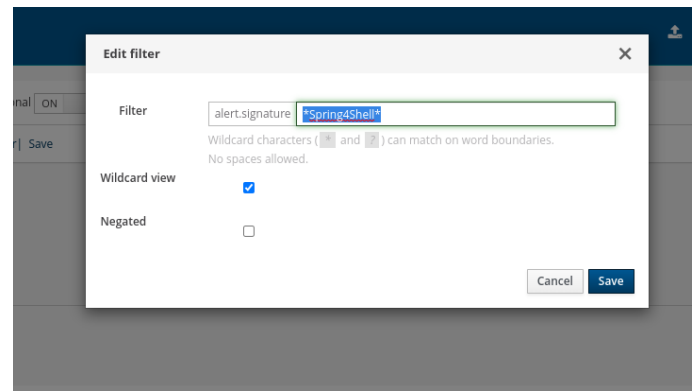
Save the Filter

NOTE: some items described here are not applicable to Stamus Probe Management license tier

The resulting filter can be saved by simply clicking on the "Save" link on the right-hand side of the "Active filter". Check "Shared" in the resulting dialog box if you want to make the filter available to all users.
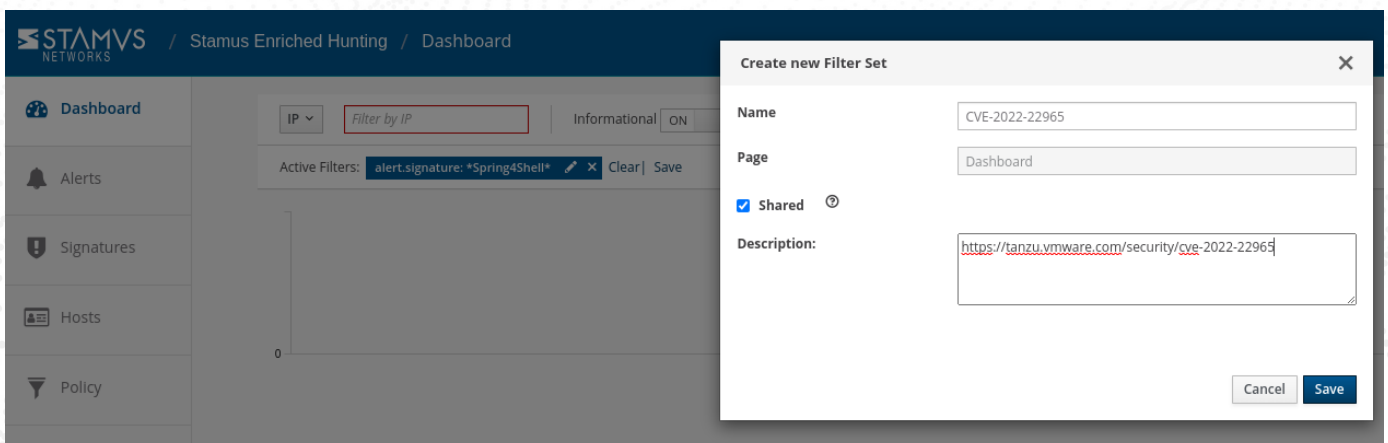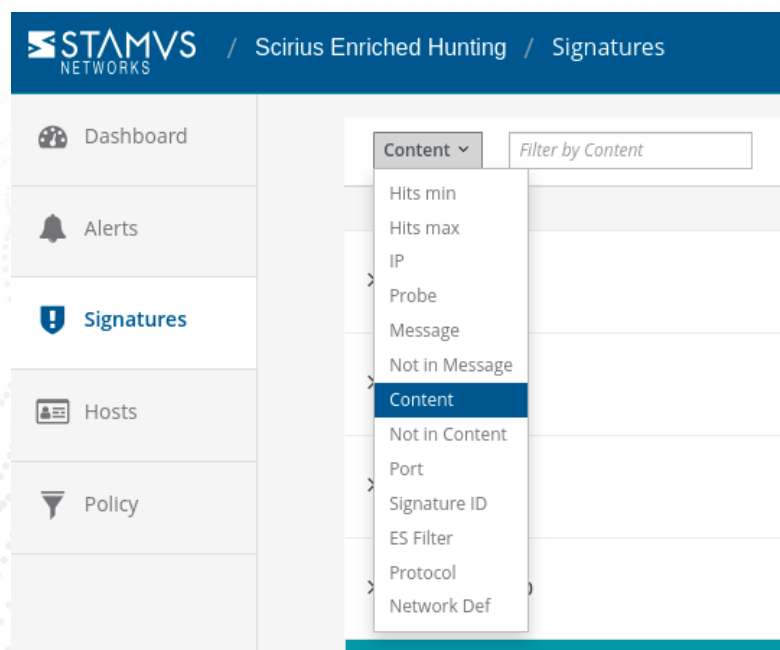
The newly created filter is now available in "Global Filter Sets" or "Private Filter Sets"
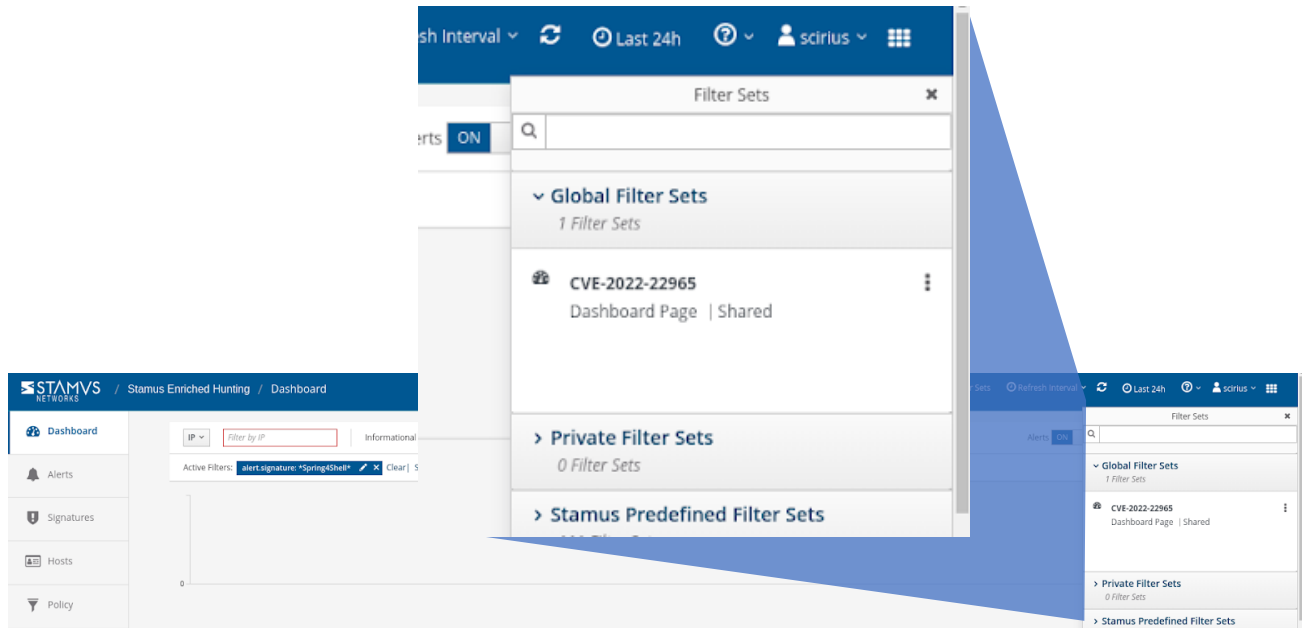
Review Detection Methods in Hunt

To review exactly what detection methods are available in Hunt for that specific vulnerability you can:

1. Head to the Signatures tab on the left-hand side in Hunt.

2. Select the "Content" option from the dropdown menu.

3. Type in the full CVE (i.e. CVE-2022-22965 or Spring4Shell), hit Enter

Automated Escalation and RestAPI Notification

NOTE: Portions are not applicable to Stamus ND or Stamus Probe Management license tiers.

If needed, an automated escalation to DoC and webhooks is also possible, including from historical data.

For example, if it happened 24hrs or 7 days ago it will still be detected and escalated based on that custom filter.

To do so:
1. After creating your filter as above
2. From the right-hand side drop down menu, *Policy Actions*, select "Create DoC events".

1. Choose the plus (+) next to the Threat: Name
2. Fill in the Threat Name, Description, and Additional information.
3. Enter an Offender Key (i.e. src_ip)
4. Enter an Asset Key (i.e. dest_ip)
5. Leave Asset Type "IP"
6. Set a Kill Chain phase (i.e. Exploit)

7. Select "Generate DoCs events from historical data". [This will make sure historical events are also checked]
8. If desired and webhooks are setup also select "Generate webhooks events from historical data"

The screenshot below shows the Declaration of Compromise event creation form:

Automated Classification and Tagging

Auto Tagging all relevant events is also an option. This will allow for any logs (alerts or protocol transaction events related to the alerts) to have a "Relevant" tag inserted in the JSON logs:

```
"tag" : "relevant"
```

To do so:

1. After creating your filter as above.
2. From the right-hand side drop down menu - Policy Actions , Select "Tag".
3. Add in an optional comment and select a ruleset.
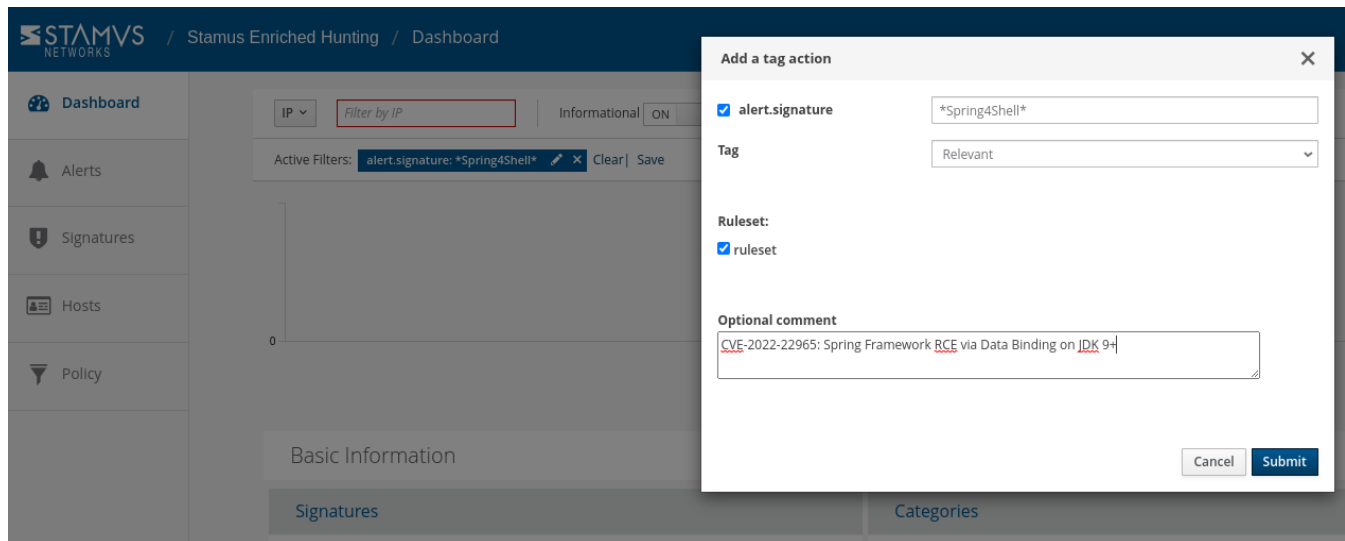
4. Update the threat detection (upload button in the middle of the top bar on the Hunt page, on the left-hand side of History, Filter Sets)

Export Data - SIEM / Elasticsearch / Kibana

All data generated by Stamus Security Platform (Stamus ND/NDR), such as alerts, protocol transactions, sightings events or Host Insights information, may be exported and shared with any SIEM or SOAR system.

Over 4000 fields are available -- from domain requests, http user agents used, hostnames, usernames logged in -- to encrypted analysis including JA3/JA3S fingerprinting, TLS certificates and more.
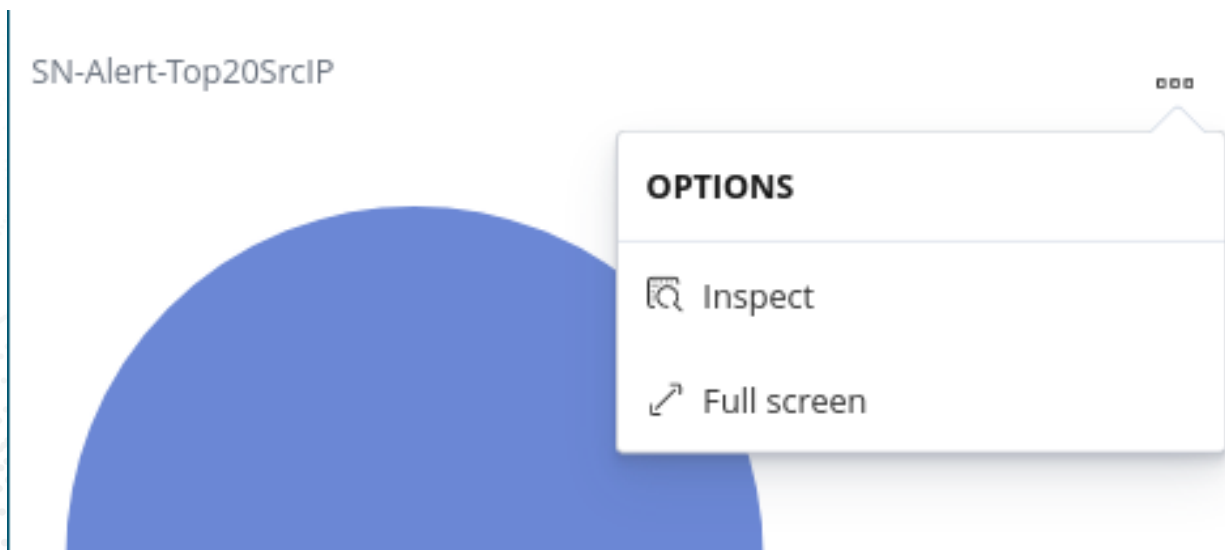
Any query of the Stamus Networks data (protocol transaction or alert logs) can be exported via a regular JSON log query or visualization export.

Example of Kibana query on alert events

To export CSV data from any info of the alerts you can open the SN-ALERT dashboard in Kibana, type in the filter "alert.signature.keyword:*Spring4Shell*" , then you can export a CSV of any visualization using "Inspect" (see example below):
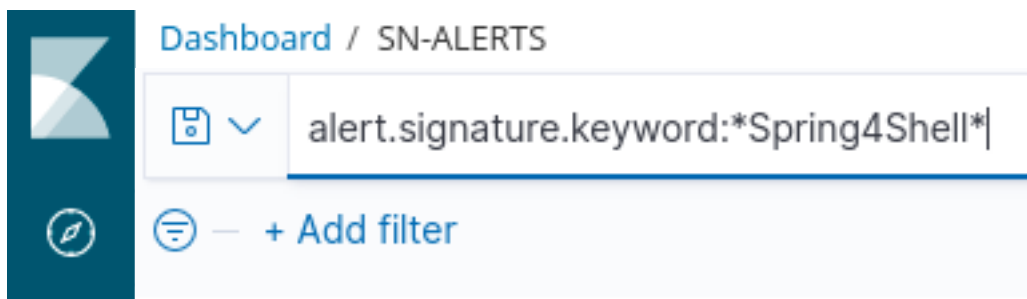
Click on "Inspect" in any visualization to export a CSV

Export Data - Spunk

NOTE: portions of this section are not applicable to Stamus Probe Management.

Any query of the Stamus Networks data (protocol transaction or alert logs a like) in Splunk can be exported via a regular Splunk query or visualization export.

Example of a Splunk query on alert events

Splunk "event_type=alert "alert.signature"="*Spring4Shell*"
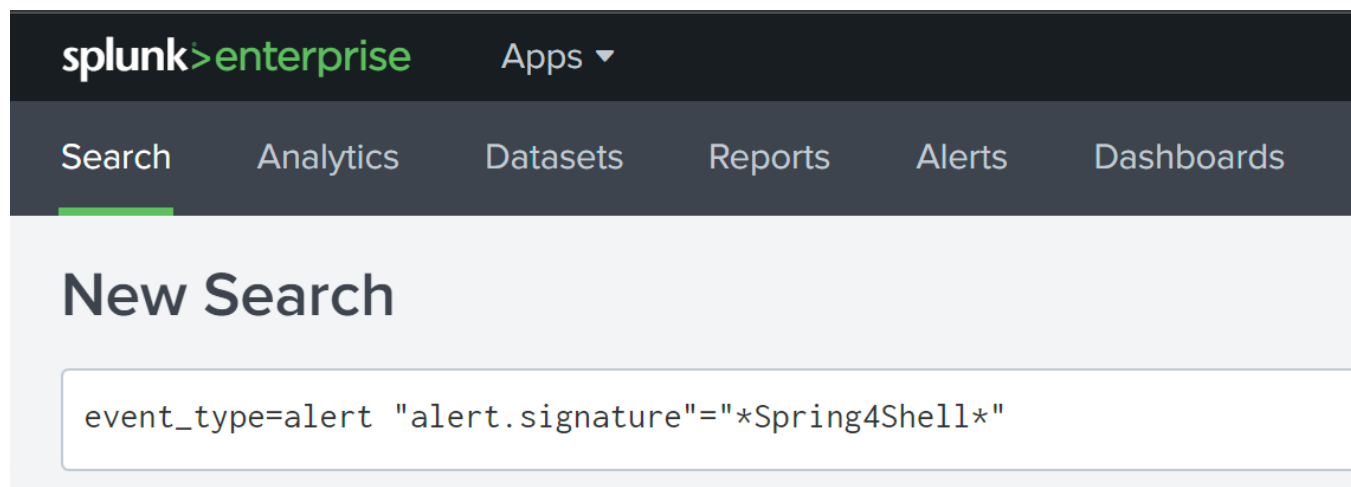
Protocol transactions

Stamus Networks provides a free Splunk app https://splunkbase.splunk.com/app/5262 that can be used to do specific CVE-2022-22963 of CVE-2022-22965 searches.

If there are any Splunk visualizations queries that have supporting information for the CVE that needs to be exported, it can be done so by the native Splunk export functionality.
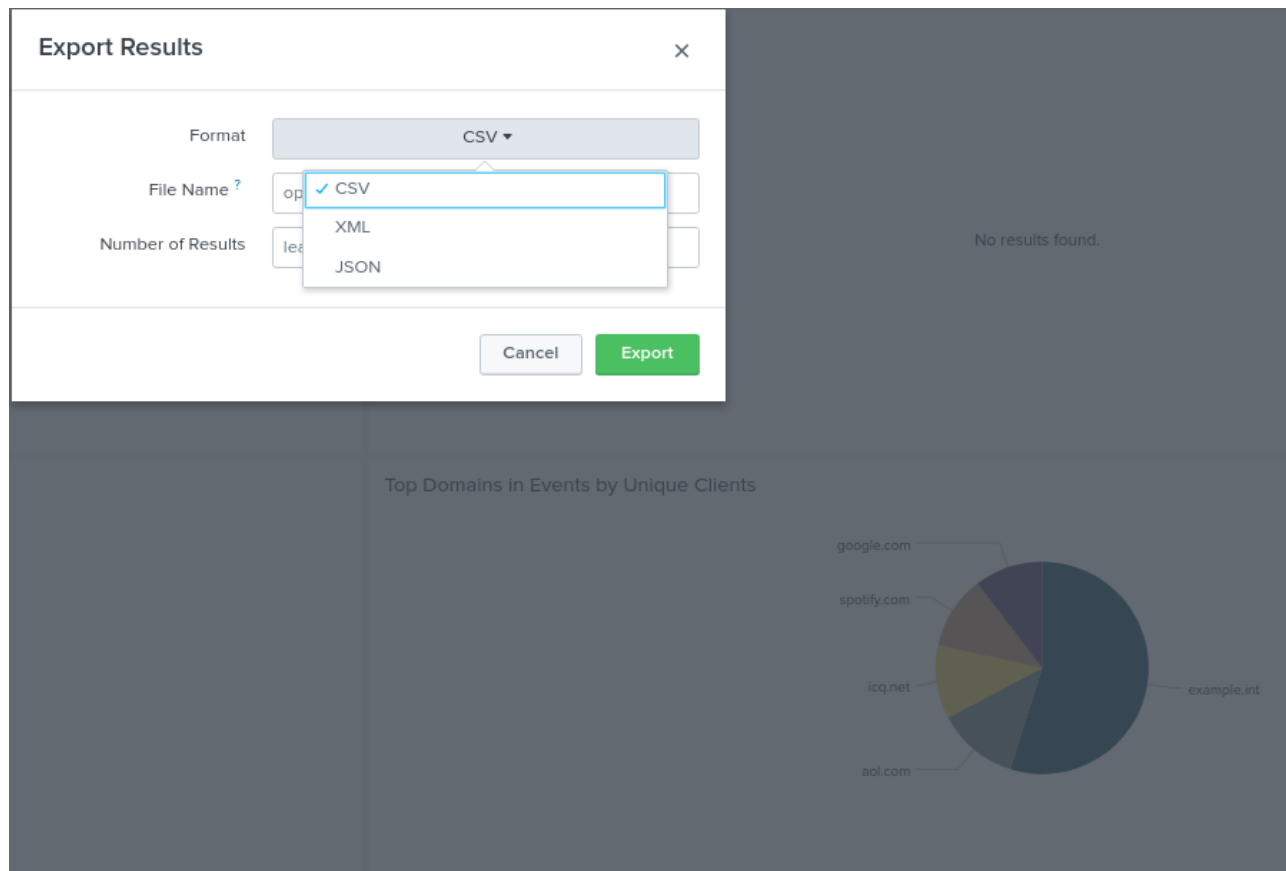
Troubleshooting and Help

Please feel free to reach out to support@stamus-networks.com with any questions or feedback.

STAMVS
NETWORKS

5 Avenue Ingres   450 E 96th St. Suite 500
75016 Paris   Indianapolis, IN 46240
France   United States

✉ contact@stamus-networks.com
🌐 www.stamus-networks.com