Splunk XSS in Save table dialog header in search page (https://splunkresearch.com/application/a974d1ee-ddca-4837-b6ad-d55a8a239c20/)

Try in Splunk Security Cloud (https://www.splunk.com/en_us/cyber-security.html)

Description

This is a hunting search to find persistent cross-site scripting XSS code that was included while inputing data in 'Save Table' dialog in Splunk Enterprise (8.1.12,8.2.9,9.0.2). A remote user with "power" Splunk role can store this code that can lead to persistent cross site scripting.

- **Type**: Hunting (https://github.com/splunk/security_content/wiki/Detection-Analytic-Types)
- **Product**: Splunk Enterprise, Splunk Enterprise Security, Splunk Cloud
- **Last Updated**: 2022-10-11
- **Author**: Rod Soto
- **ID**: a974d1ee-ddca-4837-b6ad-d55a8a239c20

Annotations

▶ ATT&CK
▶ Kill Chain Phase
▶ NIST
▶ CIS20
▶ CVE

Search

```
`splunkda` method=POST  uri=/en-US/splunkd/__raw/servicesNS/nobody/search/datamodel/model
| table _time host status clientip user uri
| `splunk_xss_in_save_table_dialog_header_in_search_page_filter`
```

Macros

The SPL above uses the following Macros:

- splunkda (https://github.com/splunk/security_content/blob/develop/macros/splunkda.yml)

> ℹ️
> ***splunk_xss_in_save_table_dialog_header_in_search_page_filter*** *is a empty macro by default. It allows the user to filter out any results (false positives) without editing the SPL.*

Required fields

List of fields required to use this analytic.

- host
- _time
- status
- clientip
- user
- uri
- method

How To Implement

Watch for POST requests combined with XSS script strings or obfuscation against the injection point /en-US/splunkd/__raw/servicesNS/nobody/search/datamodel/model.

Known False Positives

If host is vulnerable and XSS script strings are inputted they will show up in search. Not all Post requests are malicious as they will show when users create and save dashboards. This search may produce several results with non malicious POST requests. Only affects Splunk Web enabled instances.

Associated Analytic Story

- Splunk Vulnerabilities

RBA

Risk Score	Impact	Confidence	Message
25.0	50	50	Possible XSS exploitation attempt from $clientip$

> ℹ️
> *The Risk Score is calculated by the following formula: Risk Score = (Impact * Confidence/100). Initial Confidence and Impact is set by the analytic author.*

Reference

- https://www.splunk.com/en_us/product-security.html (https://www.splunk.com/en_us/product-security.html)
- https://portswigger.net/web-security/cross-site-scripting (https://portswigger.net/web-security/cross-site-scripting)

Test Dataset

Replay any dataset to Splunk Enterprise by using our `replay.py` (https://github.com/splunk/attack_data#using-replaypy) tool or the UI (https://github.com/splunk/attack_data#using-ui). Alternatively you can replay a dataset into a Splunk Attack Range (https://github.com/splunk/attack_range#replay-dumps-into-attack-range-splunk-server)

- https://raw.githubusercontent.com/splunk/attack_data/master/datasets/attack_techniques/T1189/splunk/splunk_xss_in_save_table_dialog_in_search_page.txt (https://raw.githubusercontent.com/splunk/attack_data/master/datasets/attack_techniques/T1189/splunk/splunk_xss_in_save_table_dialog_in_search_page.txt)

source (https://github.com/splunk/security_content/tree/develop/detections/application/splunk_xss_in_save_table_dialog_header_in_search_page.yml) | *version*: **1**

Tags: CVE-2022-43561 | Drive-by Compromise | Initial Access | Splunk Cloud | Splunk Enterprise | Splunk Enterprise Security

Categories: Application

Updated: October 11, 2022