Splunk Stored XSS via Data Model objectName field (https://splunkresearch.com/application/062bff76-5f9c-496e-a386-cb1adcf69871/)

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

Description

Splunk Enterprise versions 8.1.12, 8.2.9, 9.0.2 are vulnerable to persistent cross site scripting via Data Model object name. An authenticated user can inject and store arbitrary scripts that can lead to persistent cross-site scripting (XSS) in the object name Data Model.

- **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**: 062bff76-5f9c-496e-a386-cb1adcf69871

Annotations

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

Search

```
`splunkd_webx` uri=/en-US/splunkd/__raw/servicesNS/*/launcher/datamodel/model*
uri_query!=null
| stats count by _time host status clientip user uri
| `splunk_stored_xss_via_data_model_objectname_field_filter`
```

Macros

The SPL above uses the following Macros:

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

> ℹ️
> ***splunk_stored_xss_via_data_model_objectname_field_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.

- uri
- uri_query
- host
- status
- clientip
- user
- uri_path

How To Implement

This vulnerability only affects Splunk Web enabled instances. This detection does not require you to ingest any new data. The detection does require the ability to search the _internal index.

Known False Positives

This search may produce false positives and does not cover exploitation attempts via code obfuscation, focus of search is suspicious requests against "/en-US/splunkd/__raw/servicesNS/*/launcher/datamodel/model" which is the injection point.

Associated Analytic Story

- Splunk Vulnerabilities

RBA

Risk Score	Impact	Confidence	Message
25.0	50	50	A potential XSS attempt has been detected from $user$

> 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/cheat-sheet (https://portswigger.net/web-security/cross-site-scripting/cheat-sheet)

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

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

Tags: CVE-2022-43569 | Drive-by Compromise | Initial Access | Splunk Cloud | Splunk Enterprise | Splunk Enterprise Security

Categories: Application

Updated: October 11, 2022