Splunk Reflected XSS in the templates lists radio (https://splunkresearch.com/application/d532d105-c63f-4049-a8c4-e249127ca425/)

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

Description

Splunk versions below 8.1.12,8.2.9 and 9.0.2 are vulnerable to reflected cross site scripting (XSS). A View allows for a Reflected Cross Site scripting via JavaScript Object Notation (JSON) in a query parameter when ouput_mode=radio.

- **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, Chase Franklin
- **ID**: d532d105-c63f-4049-a8c4-e249127ca425

Annotations

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

Search

```
`splunkd_webx` user=admin status=200 uri=*/lists/entities/x/ui/views* uri_query!=null
| stats count earliest(_time) as event_time values(status) as status values(clientip) as clientip by index, sourcetype, _time, host, user, uri
| `splunk_reflected_xss_in_the_templates_lists_radio_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_reflected_xss_in_the_templates_lists_radio_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
- clientip
- status
- user
- uri
- uri_query
- uri_path

How To Implement

This vulnerability only affects instances with Splunk Web enabled. 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 as it is difficult to pinpoint all possible XSS injection characters in a single search string. Special attention is required to "en-US/list/entities/x/ui/views" which is the vulnerable injection point.

Associated Analytic Story

- Splunk Vulnerabilities

RBA

Risk Score	Impact	Confidence	Message
25.0	50	50	Potential XSS exploitation against radio template by $user$

> 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://research.splunk.com/stories/splunk_vulnerabilities/ (https://research.splunk.com/stories/splunk_vulnerabilities/)

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

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

Tags: CVE-2022-43568 | Drive-by Compromise | Initial Access | Splunk Cloud | Splunk Enterprise | Splunk Enterprise Security

Categories: Application

Updated: October 11, 2022