# Splunk Code Injection via custom dashboard leading to RCE (https://splunkresearch.com/application/b06b41d7-9570-4985-8137-0784f582a1b3/)

⚠️

## THIS IS A EXPERIMENTAL DETECTION

This detection has been marked experimental by the Splunk Threat Research team. This means we have not been able to test, simulate, or build datasets for this detection. Use at your own risk. This analytic is **NOT** supported.

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

## Description

This hunting search provides information about a vulnerability in Splunk Enterprise versions below 8.2.9, 8.1.12, 9.0.2, where an authenticated user can execute arbitrary code via the dashboard pdf generation component. Please review events with file=export in the _internal index for the potential targets of exploitation.

- **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**: b06b41d7-9570-4985-8137-0784f582a1b3

## Annotations

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

# Search

```
`splunkd_ui` uri_path=*/data/ui/views/* OR uri_path=*saved/searches/*
| dedup uri_path
| eval URL=urldecode("uri_path")
| rex field=URL "\/saved\/searches\/(?<NAME>[^\/]*)"
| rex field=URL "\/data\/ui\/views\/(?<NAME1>[^\/]*)"
| eval NAME=NAME."( Saved Search )",NAME1=NAME1."( Dashboard )"
| eval NAME=coalesce(NAME,NAME1)
| eval
STATUS=case(match(status,"2\d+"),"SUCCESS",match(status,"3\d+"),"REDIRECTION",match(stat
OR match(status,"5\d+"),"ERROR")
| stats list(NAME) as DASHBOARD_TITLE,list(method) as HTTP_METHOD,list(status) as
Status_Code,list(STATUS) as STATUS by user
| rename user as User
| `splunk_code_injection_via_custom_dashboard_leading_to_rce_filter`
```

# Macros

The SPL above uses the following Macros:

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

> ℹ️ ***splunk_code_injection_via_custom_dashboard_leading_to_rce_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.

- user
- clientip
- uri
- uri_path
- method
- status

## How To Implement

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

Not all exports and downloads are malicious, special attention must be put as well on /en-US/splunkd/__raw/services/pdfgen/render in the context of this search.

## Associated Analytic Story

- Splunk Vulnerabilities

## RBA

| Risk Score | Impact | Confidence | Message |
|---|---|---|---|
| 25.0 | 50 | 50 | Potential exploitation of Code Injection via Dashboard PDF generation. |

> 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)

## 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/T1210/splunk/splunk_code_injection_via_custom_dashboard_leading_to_rce.txt (https://raw.githubusercontent.com/splunk/attack_data/master/datasets/attack_techniques/T1210/splunk/splunk_code_injection_via_custom_dashboard_leading_to_rce.txt)

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

**Tags:** CVE-2022-43571 | Exploitation of Remote Services | Lateral Movement | Splunk Cloud | Splunk Enterprise | Splunk Enterprise Security

**Categories:** Application

**Updated:** October 11, 2022