Splunk Data exfiltration from Analytics Workspace using sid query (https://splunkresearch.com/application/b6d77c6c-f011-4b03-8650-8f10edb7c4a8/)

Description

This hunting search allows operator to discover attempts to exfiltrate data by executing a prepositioned malicious search ID in Analytic Workspace in Splunk Enterprise versions 8.2.9,8.1.12,9.0.2. The attack is browser-based. It requires the attacker to compel a victim to initiate a request within their browser (phishing). The attacker cannot exploit the vulnerability at will.

- **Type**: Hunting (https://github.com/splunk/security_content/wiki/Detection-Analytic-Types)
- **Product**: Splunk Enterprise, Splunk Enterprise Security, Splunk Cloud
- **Last Updated**: 2022-11-1
- **Author**: Rod Soto, Eric McGinnis
- **ID**: b6d77c6c-f011-4b03-8650-8f10edb7c4a8

Annotations

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

Search

```
`audit_searches` info=granted search NOT ("audit_searches") search NOT
("security_content_summariesonly") AND ((search="*mstats*[*]*" AND provenance="N/A") OR
(search="*mstats*\\\"*[*]*\\\"*"))
| eval warning=if(match(search,"\\\\\""), "POTENTIAL INJECTION STAGING", "POTENTIAL
INJECTION EXECUTION")
| table search, user, warning, timestamp
| `splunk_data_exfiltration_from_analytics_workspace_using_sid_query_filter`
```

Macros

The SPL above uses the following Macros:

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

> ℹ️ ***splunk_data_exfiltration_from_analytics_workspace_using_sid_query_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.

- action
- info
- user
- search_id
- metadata
- user
- _time

How To Implement

The vulnerability affects only instances with Splunk Web Enabled. After running this search, please run "Splunk Command and Scripting Interpreter Risky SPL MLTK" to gain more insight into potentially risky commands which could lead to data exfiltration.

Known False Positives

This search may produce false positives. This detection does not require you to ingest any new data. The detection does require the ability to search the _audit index. Special attention must be paid to "/en-US/app/search/analytics_workspace?sid=[sid]" which is where the malicious code will be inserted to trigger attack at victim.

Associated Analytic Story

- Splunk Vulnerabilities

RBA

Risk Score	Impact	Confidence	Message
25.0	50	50	Potential data exfiltration attack using SID query 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://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/T1567/splunk/splunk_data_exfiltration_from_analytics_workspace_using_sid_query.txt (https://raw.githubusercontent.com/splunk/attack_data/master/datasets/attack_techniques/T1567/splunk/splunk_data_exfiltration_from_analytics_workspace_using_sid_query.txt)

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

Tags: CVE-2022-43566 | Exfiltration | Exfiltration Over Web Service | Splunk Cloud | Splunk Enterprise | Splunk Enterprise Security

Categories: Application

Updated: November 1, 2022