Splunk RCE via Splunk Secure Gateway Splunk Mobile alerts feature (https://splunkresearch.com/application/baa41f09-df48-4375-8991-520beea161be/)

Description

This hunting search provides information on possible exploitation attempts against Splunk Secure Gateway App Mobile Alerts feature in Splunk versions 9.0, 8.2.x, 8.1.x. An authenticated user can run arbitrary operating system commands remotely through the use of specially crafted requests to the mobile alerts feature in the Splunk Secure Gateway app.

- **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**: baa41f09-df48-4375-8991-520beea161be

Annotations

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

Search

```
`splunkd_webx`
uri_path="/servicesNS/nobody/splunk_secure_gateway/storage/collections/data/mobile_alerts
sort="notification.created_at:-1"
| table  clientip file host method uri_query sort
| `splunk_rce_via_splunk_secure_gateway__splunk_mobile_alerts_feature_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_rce_via_splunk_secure_gateway__splunk_mobile_alerts_feature_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_path
- clientip
- file
- host
- method
- sort

How To Implement

This search only applies if Splunk Mobile Gateway is deployed in the vulnerable Splunk versions.

Known False Positives

This detection does not require you to ingest any new data. The detection does require the ability to search the _internal index. Focus of this search is "uri_path=/servicesNS/nobody/splunk_secure_gateway/storage/collections/data/mobile_al

erts*" which is the injection point.

Associated Analytic Story

- Splunk Vulnerabilities

RBA

Risk Score	Impact	Confidence	Message
81.0	90	90	Possible 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)

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

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

Tags: CVE-2022-43567 | Exploitation of Remote Services | Lateral Movement | Splunk Cloud | Splunk Enterprise | Splunk Enterprise Security

Categories: Application

Updated: October 11, 2022