# splunk - WAT scan

Report generated by Nessus™ Thu, 22 Sep 2022 10:19:24 IST

TABLE OF CONTENTS

## Vulnerabilities by Plugin


- 164076 (1) - Splunk Enterprise < 9.0 Multiple Vulnerabilities..... 4
- 164078 (1) - Splunk Enterprise and Universal Forwarder < 9.0 Improper Certificate Validation.....6
- 161707 (1) - Splunk Enterprise 8.1.x < 8.1.6 MFA Bypass.....8
- 164329 (1) - Splunk Enterprise 8.1 < 8.1.11, 8.2.0 < 8.2.7.1 / Universal Forwarders 8.1 < 8.1.11, 8..... 10
- 164272 (1) - Splunk Enterprise < 9.0.1 Information Disclosure..... 12

## Vulnerabilities by Plugin

# 164076 (1) - Splunk Enterprise < 9.0 Multiple Vulnerabilities

## Synopsis

An application running on a remote web server host is affected by multiple vulnerabilities.

## Description

The version of Splunk installed on the remote host is prior to 9.0. It is, therefore, affected by multiple vulnerabilities.

- The httplib and urllib Python libraries that Splunk shipped with Splunk Enterprise did not validate certificates using the certificate authority (CA) certificate stores by default in Splunk Enterprise versions before 9.0. Python 3 client libraries now verify server certificates by default and use the appropriate CA certificate stores for each library. Apps and add-ons that include their own HTTP libraries are not affected. (CVE-2022-32151)

- Splunk Enterprise peers in Splunk Enterprise versions before 9.0 did not validate the TLS certificates during Splunk-to-Splunk communications by default. Splunk peer communications configured properly with valid certificates were not vulnerable. However, an attacker with administrator credentials could add a peer without a valid certificate and connections from misconfigured nodes without valid certificates did not fail by default. (CVE-2022-32152, CVE-2022-32153)

- Dashboards in Splunk Enterprise versions before 9.0 might let an attacker inject risky search commands into a form token when the token is used in a query in a cross-origin request. The result bypasses SPL safeguards for risky commands. Note that the attack is browser-based and an attacker cannot exploit it at will. (CVE-2022-32154)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

## See Also

http://www.nessus.org/u?1e830af9

http://www.nessus.org/u?ad3b9d22

http://www.nessus.org/u?c6b2548f

http://www.nessus.org/u?77bc5700

## Solution

Upgrade to Splunk Enterprise 9.0, or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVSS v3.0 Temporal Score

7.9 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-32151 |
| CVE | CVE-2022-32152 |
| CVE | CVE-2022-32153 |
| CVE | CVE-2022-32154 |
| XREF | IAVA:2022-A-0251-S |

Plugin Information

Published: 2022/08/11, Modified: 2022/08/31

Plugin Output

192.168.151.126 (tcp/8000/www)

```
URL               : http://cpt-price:8000/
Installed version : 8.1.1
Fixed version     : 9.0
```

## 164078 (1) - Splunk Enterprise and Universal Forwarder < 9.0 Improper Certificate Validation

### Synopsis

An application running on a remote web server host is affected by an improper certificate validation vulnerability.

### Description

In Splunk Enterprise and Universal Forwarder versions before 9.0, the Splunk command-line interface (CLI) did not validate TLS certificates while connecting to a remote Splunk platform instance by default. Splunk peer communications configured properly with valid certificates were not vulnerable. However, connections from misconfigured nodes without valid certificates did not fail by default.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

http://www.nessus.org/u?4d24490e

### Solution

Upgrade Splunk Enterprise or Universal Forwarder to version 9.0 or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

### CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

### CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

### STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2022-32156 |
| XREF | IAVA:2022-A-0251-S |

## Plugin Information

Published: 2022/08/11, Modified: 2022/08/31

## Plugin Output

192.168.151.126 (tcp/8000/www)

```
URL              : http://cpt-price:8000/
Installed version : 8.1.1
Fixed version     : 9.0
```

# 161707 (1) - Splunk Enterprise 8.1.x < 8.1.6 MFA Bypass

## Synopsis

An application running on a remote web server host may be affected by an MFA bypass vulnerability.

## Description

According to its self-reported version number, the version of Splunk running on the remote web server is Splunk Enterprise 8.1.x prior to 8.1.6. It is, therefore, affected by a vulnerability in Splunk Enterprise's implementation of DUO MFA that allows for bypassing the MFA verification. The vulnerability impacts Splunk Enterprise instances configured to use DUO MFA and does not impact or affect a DUO product or service.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

## See Also

http://www.nessus.org/u?52d93bf3

## Solution

Upgrade Splunk Enterprise to version 8.1.6, 8.2.0, or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

## CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/RL:O/RC:C)

## CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

## CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2021-26253 |
| XREF | IAVA:2022-A-0219-S |

## Plugin Information

Published: 2022/05/31, Modified: 2022/09/05

## Plugin Output

192.168.151.126 (tcp/8000/www)

```
URL               : http://cpt-price:8000/
Installed version : 8.1.1
Fixed version     : 8.1.6 / 8.2.0
```

## 164329 (1) - Splunk Enterprise 8.1 < 8.1.11, 8.2.0 < 8.2.7.1 / Universal Forwarders 8.1 < 8.1.11, 8.2.0 < 8.2.7.1 (SVD-2022-0803)

### Synopsis

An application running on a remote web server host is affected by a vulnerability

### Description

The version of Splunk installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the SVD-2022-0803 advisory.

- In Splunk Enterprise and Universal Forwarder versions in the following table, indexing a specially crafted ZIP file using the file monitoring input can result in a crash of the application. Attempts to restart the application would result in a crash and would require manually removing the malformed file.

(CVE-2022-37439)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

http://www.nessus.org/u?06538c78

### Solution

For Splunk Enterprise and Universal Forwarder customers, upgrade versions to 8.1.11, 8.2.7.1, or higher.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

### CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

### CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| CVE | CVE-2022-37439 |
| XREF | CWE:409 |

## Plugin Information

Published: 2022/08/22, Modified: 2022/08/22

## Plugin Output

192.168.151.126 (tcp/8000/www)

```
URL               : http://cpt-price:8000/
Installed version : 8.1.1
Fixed version     : 8.1.11
```

## 164272 (1) - Splunk Enterprise < 9.0.1 Information Disclosure

### Synopsis

An application running on a remote web server host may be affected by an information disclosure vulnerability.

### Description

Splunk Enterprise versions in the following table, an authenticated user can craft a dashboard that could potentially leak information (for example, username, email, and real name) about Splunk users, when visited by another user through the drilldown component. The vulnerability requires user access to create and share dashboards using Splunk Web.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

http://www.nessus.org/u?378d3c80

### Solution

Upgrade Splunk Enterprise to version 8.1.11, 8.2.7.1, 9.0.1, or later.

### Risk Factor

Low

### CVSS v3.0 Base Score

3.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N)

### CVSS v3.0 Temporal Score

3.1 (CVSS:3.0/E:U/RL:O/RC:C)

### CVSS v2.0 Base Score

2.1 (CVSS2#AV:N/AC:H/Au:S/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

1.6 (CVSS2#E:U/RL:OF/RC:C)

### STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2022-37438 |
| XREF | IAVA:2022-A-0333 |

## Plugin Information

Published: 2022/08/18, Modified: 2022/08/31

## Plugin Output

192.168.151.126 (tcp/8000/www)

```
URL               : http://cpt-price:8000/
Installed version : 8.1.1
Fixed version     : 8.1.11
```