

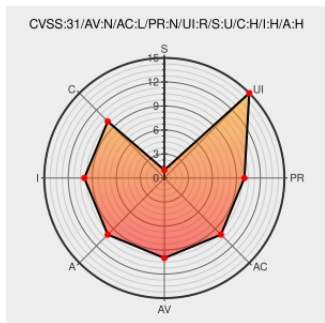


# CVE-2022-27183

Published on: Not Yet Published

Last Modified on: 05/14/2022 02:25:00 AM UTC

## CVE-2022-27183 - advisory for SVD-2022-0505

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Splunk](#) from [Splunk](#) contain the following vulnerability:

The Monitoring Console app configured in Distributed mode allows for a Reflected XSS in a query parameter in Splunk Enterprise versions before 8.1.4. The Monitoring Console app is a bundled app included in Splunk Enterprise, not for download on SplunkBase, and not installed on Splunk Cloud Platform instances. Note that the Cloud Monitoring Console is not impacted.

CVE-2022-27183 has been assigned by prodsec@splunk.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Splunk - Splunk Enterprise** version **Version(s) before 8.1.4**

CVSS3 Score: **6.1 - MEDIUM**

| Attack Vector  | Attack Complexity      | Privileges Required | User Interaction    |
|----------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b> | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope          | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>CHANGED</b> | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>PARTIAL</b>    | <b>NONE</b>         |

## CVE References

| Description | Tags | Link |
|-------------|------|------|
|-------------|------|------|

Splunk XSS in Monitoring Console - Splunk Security Content

[research.splunk.com](https://research.splunk.com/text/html)  
text/html

 MISC  
[research.splunk.com/application/splunk\\_xss\\_in\\_monitoring\\_console/](https://research.splunk.com/application/splunk_xss_in_monitoring_console/)

SVD-2022-0505 | Splunk

[www.splunk.com](https://www.splunk.com/text/html)  
text/html

 MISC [www.splunk.com/en\\_us/product-security/announcements/svd-2022-0505.html](https://www.splunk.com/en_us/product-security/announcements/svd-2022-0505.html)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

Related QID Numbers

378054 Splunk Enterprise Reflected Cross-Site Scripting (XSS) Vulnerability in Monitoring Console (SVD-2022-0505)

Known Affected Configurations (CPE V2.3)

| Type        | Vendor                 | Product                | Version | Update | Edition | Language |
|-------------|------------------------|------------------------|---------|--------|---------|----------|
| Application | <a href="#">Splunk</a> | <a href="#">Splunk</a> | All     | All    | All     | All      |

cpe:2.3:a:splunk:splunk:\*:\*:\*:enterprise:\*:\*:

Discovery Credit

Danylo Dmytriiev (DDV\_UA)

Social Mentions

| Source                                                                                        | Title                                                                                                                                                                                                    | Posted (UTC)        |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|  @CVEreport | CVE-2022-27183 : The Monitoring Console app configured in Distributed mode allows for a Reflected #XSS in a query p... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-05-06 17:06:05 |
|  /r/netcve  | <a href="#">CVE-2022-27183</a>                                                                                                                                                                           | 2022-05-06 18:38:35 |

← Previous ID

Next ID →