

---

# 0-day Vulnerabilities in Spring (Spring4Shell, CVE-2022-22963, and CVE-2022-22965)

## Summary

On Tuesday, March 29, news of potential vulnerabilities in the Spring Framework was surfaced. The Spring Framework is a very popular framework used by Java developers to build modern applications and is owned by VMware.

Spring is providing regular updates via its support blog: <https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement> (<https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement>)

We have not received any reports of these issues from SolarWinds customers but are actively investigating. The following SolarWinds products do utilize the Spring Framework, but have not yet been confirmed to be affected by this issue:

- Security Event Manager (SEM)
- Database Performance Analyzer (DPA)
- Web Help Desk (WHD)

**We have confirmed all other SolarWinds products ARE NOT AFFECTED by this issue, including the Orion Platform and its modules.**

Information about the CVEs associated with these issues are available at <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22963> and <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965>.

Spring has also announced a new CVE-2022-22947 which is specific to the Spring Cloud product. SolarWinds products are not affected by this vulnerability.

While we have not seen or received reports of SolarWinds products affected by this issue, for the protection of their environments, **SolarWinds strongly recommends all customers disconnect their public-facing (internet-facing) installations of these SolarWinds products (SEM, DPA and WHD) from the internet.**

On March 31, we previously indicated Virtualization (VMAN) Poller (an internally facing component **only**) was being evaluated, due to its use of the Spring Framework. We have now confirmed **VMAN is not affected by this issue**.

Additionally, we recommend users of these products ensure they are referencing our best practices and recommendations as follows:

- **Security Event Manager (SEM):** Please review the *Secure SEM* section of *SEM Administrator Guide* ([https://documentation.solarwinds.com/en/success\\_center/sem/content/sem\\_administrator\\_guide.htm](https://documentation.solarwinds.com/en/success_center/sem/content/sem_administrator_guide.htm))
- **Database Performance Analyzer (DPA):** Please review the *DPA Secure Configuration Guide Best Practices and Recommendations* ([https://support.solarwinds.com/SuccessCenter/s/article/DPA-Secure-Configuration-Guide-Best-Practices-and-Recommendations?language=en\\_US](https://support.solarwinds.com/SuccessCenter/s/article/DPA-Secure-Configuration-Guide-Best-Practices-and-Recommendations?language=en_US))

SolarWinds is actively investigating these newly reported vulnerabilities and will provide regular updates as new information becomes available and is validated. Out of an abundance of caution, we have released updates to these products to include the latest version of the Spring Framework the Spring team made available March 31.

The hotfixes for both Database Performance Analyzer (DPA), Security Event Manager (SEM), and Web Help Desk (WHD) are all now available in your Customer Portal. The hotfix for the Security Event Manager (SEM) is currently anticipated to be available the week of April 10. We will notify customers when each of these updates are available.

## Affected Products

- Security Event Manager (SEM)
- Database Performance Analyzer (DPA)
- Web Help Desk (WHD)

## Fixed Software Release

- Database Performance Analyzer 2022.1.7779  
([https://documentation.solarwinds.com/en/success\\_center/dpa/content/release\\_notes/dpa\\_2022-1-7779\\_release\\_notes.htm](https://documentation.solarwinds.com/en/success_center/dpa/content/release_notes/dpa_2022-1-7779_release_notes.htm))
- ([https://documentation.solarwinds.com/en/success\\_center/dpa/content/release\\_notes/dpa\\_2022-1-7779\\_release\\_notes.htm](https://documentation.solarwinds.com/en/success_center/dpa/content/release_notes/dpa_2022-1-7779_release_notes.htm)) Web Help Desk 12.7.8 HF2  
([https://support.solarwinds.com/SuccessCenter/s/article/Web-Help-Desk-12-7-8-Hotfix-2-Release-Notes?language=en\\_US](https://support.solarwinds.com/SuccessCenter/s/article/Web-Help-Desk-12-7-8-Hotfix-2-Release-Notes?language=en_US))
- Security Event Manager 2022.2  
([https://documentation.solarwinds.com/en/success\\_center/sem/content/release\\_notes/sem\\_2022-2\\_release\\_notes.htm](https://documentation.solarwinds.com/en/success_center/sem/content/release_notes/sem_2022-2_release_notes.htm))

---

### Advisory Details

#### Severity

N/A

**Advisory ID**

CVE-2022-22963 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22963>)

CVE-2022-22965 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965>)

**First Published**

03/31/2022

**Last Updated**

04/11/2022

**Version**

00.000

**Workarounds**

No workarounds available

**Bugs IDs**

N/A

**CVSS Score**

N/A

