Product Security Advisory

# HID SAFE – Yellowfin and SpringShell

TLP:WHITE

No restriction on distribution

**HID-PSA-2022-<index>**

2022-April-29

**Severity:** **CRITICAL** - CVSS 9.8 (3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

## Overview:

A critical vulnerability, named SpringShell, has been identified as CVE-2022-22965 and could potentially lead to a remote code execution attack. This vulnerability affects HID SAFE when using the SAFE Reports functionality which uses a Yellowfin software component. Note that this is an optional component that can be selected during installation.

## Affected Products:

**HID SAFE** versions 5.13 to version 5.17 where SAFE Reports (Yellowfin version 9.2) is installed.

## Impact:

If SAFE Reports (Yellowfin) is installed on the affected version, an attacker may be able to remotely send a request to Yellowfin and execute malicious code.

## Mitigation:

We recommend updating the affected Spring dependencies used by Yellowfin to the latest version:

1. Download spring-5.3.18.zip from https://ftp.yellowfin.bi/f/9cfd967ef889adce
2. Stop the SAFE Reporting server service.
3. Remove the vulnerable Spring dependencies from the C:\SAFEReporting\appserver\webapps\reporting\WEB-INF\lib folder (libraries that match spring-*.jar)

- spring-aop-5.1.4.RELEASE.jar
- spring-beans-5.1.4.RELEASE.jar
- spring-context-5.1.4.RELEASE.jar
- spring-context-support-5.1.4.RELEASE.jar
- spring-core-5.1.4.RELEASE.jar
- spring-expression-5.1.4.RELEASE.jar
- spring-web-5.1.4.RELEASE.jar
- spring-webmvc-5.1.4.RELEASE.jar
- spring-websocket-5.1.4.RELEASE.jar

4. Unzip the downloaded file, copy the new Spring dependencies into the C:\SAFEReporting\appserver\webapps\reporting\WEB-INF\lib folder.
    - spring-aop-5.3.18.jar
    - spring-beans-5.3.18.jar
    - spring-context-5.3.18.jar
    - spring-context-support-5.3.18.jar
    - spring-core-5.3.18.jar
    - spring-expression-5.3.18.jar
    - spring-web-5.3.18.jar
    - spring-webmvc-5.3.18.jar
    - spring-websocket-5.3.18.jar
5. Restart SAFE Reporting server service.

NOTE: Mitigation steps are based on Yellowfin remediation steps found here - https://community.yellowfinbi.com/knowledge-base/article/yellowfin-and-the-springshell-vulnerability

## Contact Information:

If you have additional questions, please contact your HID Global representative.

If you suspect that an HID Global product has been the target of an attack, please contact HID Technical Support at https://www.hidglobal.com/support.