SPRING4SHELL VULNERABILITY ANNOUNCEMENT

We are aware that there is a vulnerability in Sprint Framework called Spring4Shell which was assigned the following CVEs:

- CVE-2022-22965
- CVE-2022-22963

Vulnerable

Only CVE-2022-22965 is affecting SAFEQ.
Only YSoft SAFEQ 6 build 30 or newer is affected.

YSoft SAFEQ 6 Subsystems affected:

- **End User Interface (EUI):** has a vulnerable library, using Valve access logger, probably exploitable by public exploit (spring-beans version 4.x)
- **Payment System (YPS):** has a vulnerable library, using Valve access logger, probably exploitable by public exploit (spring-beans version 4.x)
- **Payment System plugins:** has vulnerable library, using Valve access logger, probably exploitable by public exploit (spring-beans version 4.x)
- **Product extensions:**
  - SWC-140 - Sogecommerce Payment Gateway
  - SWC-122 - Web-Based Card Management
  - SWC-119 - Multi-Level Reports
  - SWC-114 - Guest accounts self-registration web portal
  - SWC-113 - Zapper Payment Gateway Integration
  - SWC-109 - DIBS Easy Payment Gateway
  - SWC-105 - Offline accounting in combination with YSoft Payment System
  - SWC-83 - MultiSafepay Payment Gateway
  - SWC-81 - OneStopSecure Payment Gateway
  - SWC-75 - YSoft All Jobs (print, scan and copy) Archiving, full-text Search and keyword Triggers (YAJAST)
  - SWC-73 - My Savings Data
  - SWC-49 - Web interface for delegated print queue management

- Not exploitable but contains a vulnerable Spring version:

  - **Management**: has a vulnerable library, but the public exploit doesn't work (not using Valve access logger) (spring-beans version 5.3)

  - **Infrastructure Management Service (IMS 1.4):** has a vulnerable library, but the public exploit doesn't work (not using Valve access logger) (spring-beans version 4.x)

Not Vulnerable

- YSoft SAFEQ 6 Build 67 or newer
- YSoft SAFEQ 6 Build 29 or older
- SAFEQ Cloud (fixed under standard emergency release process by April 8, 2022)
- YSoft SAFEQ 5
- YSoft SAFEQ 4
- YSoft SAFEQ Mobile Integration Gateway
- YSoft SAFEQ Mobile Print Server
- YSoft SAFEQ Client (SAFEQ 5 client)
- YSoft SAFEQ Client v3
- FlexiSpooler
- Mobile terminal
- YSoft SAFEQ Embedded Terminals
- Local Monitor
- YSoft Card Reader Tool (and usbrtool.exe)
- YSoft IPP testing tool
- Data Protection Tool included in SAFEQ 6 (all versions)
- YSoft BE3D™ DeeControl 2

Resolution

1. Apply a patch
   - Download the SpringPatcher tool and follow README document that is included in the same archive.
   - *Note: SpringPatcher restarts Payment System (YPS), this will cause temporary unavailability and can interrupt some printing/copying/scanning operations in the environment where this component is utilized (e.g., for prepaid accounts or quotas).*
   - *Latest version:* v14 (released 08 Apr 2022)
   - *Download link:* bit.ly/3DSEbLi
2. Update product extensions
   Note: All the vulnerable extensions were fixed. The versions listed below already contain the fix.
   Note: If the extension is not publicly available on Partner Portal, kindly contact your Regional Sales Manager in order to obtain its new version.

   - SWC-140 - Sogecommerce Payment Gateway (v1.2)
   - SWC-122 - Web-Based Card Management (v1.2)
   - SWC-119 - Multi-Level Reports (v1.11)
   - SWC-114 - Guest accounts self-registration web portal (v1.17)

- SWC-113 - Zapper Payment Gateway Integration (v1.2)
- SWC-109 - DIBS Easy Payment Gateway (v1.10)
- SWC-105 - Offline accounting in combination with YSoft Payment System (v1.10)
- SWC-83 - MultiSafepay Payment Gateway (v1.9)
- SWC-81 - OneStopSecure Payment Gateway (v1.3)
- SWC-75 - YSoft All Jobs (print, scan and copy) Archiving, full-text Search and keyword Triggers (YAJAST) (v2.35)
- SWC-73 - My Savings Data (1.5)
- SWC-49 - Web interface for delegated print queue management (v1.16)

Next Releases

YSoft SafeQ Build 68

Build 67 and Build 68 are not vulnerable anymore. The vulnerability is mitigated in the code but the Spring Framework is not updated yet, which means some security scanners may still raise a false detection about the vulnerability presence. For more details about mitigation steps and false detection, refer to the FAQ section.

- Build 67 released on April 7, 2022.
- Build 68 is available by April 21, 2022.

All Spring Framework components will be updated to the recent version in one of the upcoming releases to prevent false positive detection by security scanners.