SPRING4SHELL VULNERABILITY ANNOUNCEMENT

We are aware that there is a vulnerability in Sprint Framework called Spring4Shell. The most discussed vulnerabilities are CVE-2022-22965/Spring4Shell (Spring Core). We will keep this post updated.

Vulnerable

YSoft SAFEQ 6 Build 30 or newer

- **Management**: has a vulnerable library, but the public exploit doesn't work (not using Valve access logger) (spring-beans version 5.3)
- **End User Interface (EUI)**: has a vulnerable library, using Valve access logger, probably exploitable by public exploit (spring-beans version 4.x)
- **Y Soft Payment System (YPS)**: has a vulnerable library, using Valve access logger, probably exploitable by public exploit (spring-beans version 4.x)
- **YPS plugins**: has vulnerable library, using Valve access logger, probably exploitable by public exploit (spring-beans version 4.x)
- **Infrastructure Management Service (IMS 1.4)**: has vulnerable library, but public exploit doesn't work (not using Valve access logger) (spring-beans version 4.x)

Product extensions:

- **YPS plugins**: has a 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 Vulnerable

- YSoft SAFEQ 6 Build 29 or older
- 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
-

You can find the latest mitigation steps below.

Mitigation

DO THIS NOW – Apply the Patch

Download the SpringPatcher tool and follow the attached README document.

- bit.ly/3LKmFLV

Next Release – With the patch included

Dispatcher Paragon Build 67 and Dispatcher Paragon Build 68 will not be vulnerable anymore. The Spring Framework will not be updated yet but the vulnerability will be mitigated in the code.

- Build 67 will be available as originally planned.
- Build 68 will be available as originally planned.

Notes: we use the recommended workaround (https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement#disallowed-fields) to prevent access to the class loader from the form input field. Security scans can still raise alarm but in this release, it's a false positive.

Next Release – Spring Framework is updated on all components

Dispatcher Paragon Build 69 will be released with all Sprint Framework components updated and the vulnerability completely removed. Release date is as planned.