1 Advisory Information

- **Advisory ID:** BOSCH-SA-309239-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2022-22965
    - Base Score: 9.8 (Critical)
- **Published:** 27 Apr 2022
- **Last Updated:** 27 Apr 2022

2 Summary

The access control and time attendance management software Bosch MATRIX uses a version of the Java Spring Framework that is vulnerable to "spring4shell" (CVE-2022-22965). Bosch MATRIX does NOT use a configuration that is currently known to be exploitable using this vulnerability, but as the developers of Spring point out, other attack vectors to exploit this vulnerability may exist. Therefore we recommend updating the vulnerable components to be on the safe side.

A vulnerable version of the Spring Framework is used in Bosch MATRIX versions 3.3, 3.4, 3.5, 3.6, 3.7 up to and including 3.7.6 and 3.8 up to and including 3.8.4. A security patch to update the affected components for the currently supported versions of Bosch MATRIX (3.7 and 3.8) is available. In addition, the components will automatically be updated in the next minor release for these versions (3.7.7 and 3.8.5 respectively), as well as in the upcoming major release (3.9). Older versions of Bosch MATRIX (3.6 and lower) have to be upgraded to a supported version of Bosch MATRIX first in order to be able to close this vulnerability.

3 Affected Products

- Bosch MATRIX >= 3.3
- Bosch MATRIX <= 3.6
- Bosch MATRIX <= 3.7.6
- Bosch MATRIX <= 3.8.4

4 Solution and Mitigations

4.1 Install Security Patch for the Affected Components

We recommend installing the security patch to replace the vulnerable Spring Framework components with a fixed version. The patch is available for the supported Bosch MATRIX versions 3.7 and 3.8. Please contact the Bosch Building Technologies Integrator Business Service Hotline if you require the necessary patch files (contact details are included in the acceptance documentation of your solution).

When installing the security patch the MATRIX software is stopped for about a minute, which temporarily prevents changes to the system. After substitution of the affected components the security patch installation routine automatically restarts the MATRIX software. In most cases no impact on the access control and/or time attendance system is to be expected, since the access control terminals cache access authorizations locally.

Successful installation of the security patch can be verified by checking the version number of the Spring framework components in the following path (assuming the software is installed in the default location). The version number at the end of the file names should be at least 5.3.18:

```
C:\Program Files\BOSCH\MATRIX\main\webapps\matrix\WEB-INF\lib\spring-*.jar
```

4.2 Install Upcoming Release

The upcoming releases of Bosch MATRIX will automatically update the affected components during the installation. The following versions will include the updated Spring Framework library:

- Bosch MATRIX version 3.7.7 (expected early June 2022)
- Bosch MATRIX version 3.8.5 (expected end of May 2022)
- Bosch MATRIX version 3.9 (expected mid May 2022)

5 Vulnerability Details

5.1 CVE-2022-22965

CVE description: A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

- Problem Type:
  - CWE-94: Improper Control of Generation of Code ('Code Injection')
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

6 Remarks

6.1 Security Update Information

With respect to Directive (EU) 2019/770 and Directive (EU) 2019/771 and their national transposition laws, please note:

It is your responsibility to download and/or install any security updates provided by us, for example to maintain product or data security. If you fail to install a security update provided to you within a reasonable period of time, we will not be liable for any product defect solely due to the absence of such security update.

Alternatively, we are entitled to directly download and/or install security updates regardless of your settings. In these cases, we will provide you with the relevant information, e.g. in this security advisory.

6.2 CVSS Scoring

Vulnerability classification has been performed using the CVSS v3.1 scoring system. The CVSS environmental score is specific to each customer's environment and should be defined by the customer to attain a final scoring.

7 Additional Resources

- [1] Spring Framework RCE Announcement: https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

Please contact the Bosch PSIRT if you have feedback, comments, or additional information about this vulnerability at: psirt@bosch.com.

8 Revision History

- 27 Apr 2022: Initial Publication

9 Appendix

9.1 Material List

SAP#	Product Description
F.01U.569.235	MATRIX Software 3000
F.01U.569.236	MATRIX Software 5000
F.01U.579.309	MATRIX Zeitwirtschaft für 100 MA
F.01U.586.811	MATRIX Zeitwirtschaft für 50 MA
F.01U.591.875	MATRIX Software 2000 EMA