7SIGNAL Inc.
6155 Rockside Drive Suite 110
Independence, OH 44131
(216) 777 – 2900

Cloud Operations CYBERSECURITY Vulnerability Report

IML3-947 (CVE-2022-22965)

Date and time incident began: April 8, 2022

Date and time incident ended: April 14, 2022 (planned at time of issued document)

Published Vulnerability:
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.

Impact identified vulnerability:

- Sapphire Eye using version 4.3.2 no impact or risk.
- Sapphire Eye hardware not using Spring Framework.
- Mobile Eye web application not using Spring Framework.
- Mobile Eye Agents Using 5.2.3 (no risk not a web server).
- Production System tested for all Spring Framework products with no risks identified.
- SIEM logs showed no signs of exploitation.

Resolution:

- Sapphire Eye will update to a more current version in Q2 or Q3 2022 as planned in the technical roadmap.
- Mobile Eye Agent will upgrade to 5.3.18 by 4/15/2022 once tested to ensure no new issues are introduced into Production.
- Mobile Eye Agent.
- No loss of data.
- No security breach or risk was introduced.

Procedural or Design changes planned:

- Continue to run vulnerability testing with 3rd party tools (per 7SIGNAL policy).
- Continue to monitor https://nvd.nist.gov/vuln/detail/cve-2022-22965 for future update.
- Reviewed Incident with 7SIGNAL CTO.