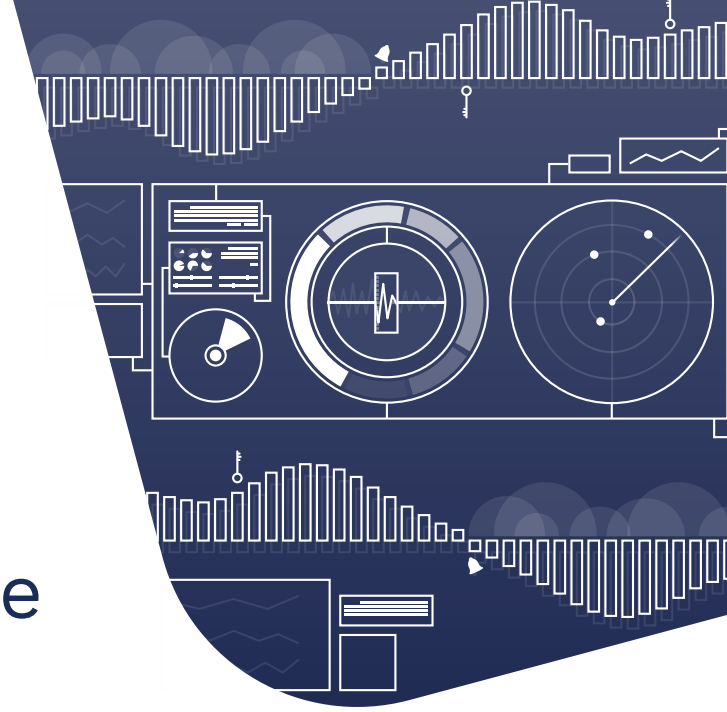
KUDELSKI IOT THINGS



Continuous Firmware Monitoring

We help companies keep their devices and firmware within their defined security target throughout their entire lifecycle, enabling them to comply with post-market surveillance requirements. Master the vulnerability exposure of your firmware and be notified when there are new threats to your device.

CONTEXT

Increase in discovered Common Vulnerabilities and Exposures (CVE)

With an increase in discovered Common Vulnerabilities and Exposures (CVE) to almost 22,000 in 2021, benchmarking IoT devices running software against recent and constantly evolving threats appears mandatory.

Last year, 20% of the reported vulnerabilities were registered as High or Critical, impacting systems in a major way if exploited.

CVSS Score	Number of Vulnerabilities	Percentage
0 - 1	673	3.10%
1 - 2	90	0.40%
2 - 3	1,245	5.70%
3 - 4	1,917	8.80%
4 - 5	5,942	27.30%
5 - 6	3,691	17.00%
6 - 7	3,893	17.90%
7 - 8	3,065	14.10%
8 - 9	123	0.60%
9 - 10	1,131	5.20%
Total	**21,770**	**100%**

Weighted Average CVSS Score: 5.9

Distribution of all vulnerabilities by CVSS score

APPROACH

Continuous firmware monitoring capabilities

Our firmware monitoring capabilities and IoT security expertise give you a clear understanding of how your system measures against recent and relevant threats.

> “Armed with this knowledge, you can prepare more efficient critical updates and remediations

Identification of relevant risks

Sorting through the numerous alerts raised regularly for your IoT system, we identify potential attack vectors, filtering out attacks with limited effect or too difficult to implement. This results in a comprehensive view of relevant new risks that your products should be protected against.

Full confidentiality level

The Continuous Firmware Monitoring runs on-premises in our secure building in Switzerland to ensure we maintain a controlled confidentiality level. The monitoring is enriched with threat intelligence from Shodan and the NIST NVD.

Supported platforms

Unencrypted firmware file, update file, or flash dump, including archives, filesystems, and compressed data are supported for most of the IoT hardware platforms and OS. Further insights are provided with Linux-based platforms.

CORE INGREDIENTS

Typical vulnerabilities under monitoring

1. 3rd-party components (software composition analysis) and thousands of known vulnerabilities
2. Default or undocumented credentials (often exploited by “Mirai” and other bots)
3. Hardcoded cryptographic secrets (including certificates and private keys)
4. Leftover development or backdoor accounts
5. Vulnerable service configuration

INCLUDED

Support level adapted to your monitoring needs

- Daily firmware scan
- Daily update of CVE database
- 1 year of monitoring, renewable
- 4 firmware updates included
- Security Expert analysis

> “Benefit from Kudelski IoT’s unparalelled security and monitoring expertise, on demand or through your whole IoT journey

 V1.6