BUGPROVE

Product Security

for the Internet of Things

BugProve

sales@bugprove.com

https://bugprove.com/

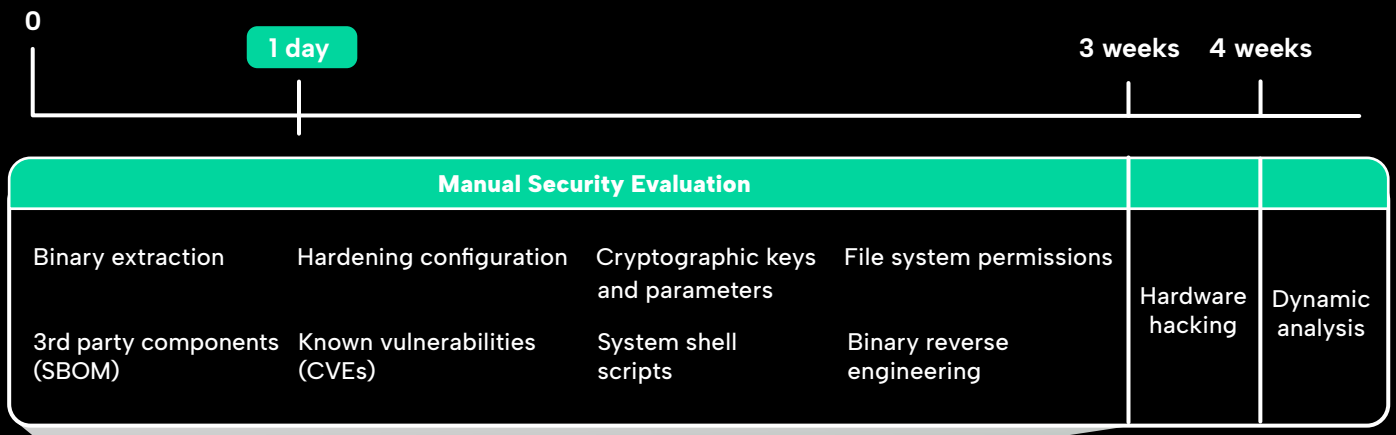
BUGPROVE

OUR PITCH

While the application security domain already has several available tools and solutions (like SCA, SAST or DAST), there is still no comprehensive, out-of-the-box platform to automate security tasks for IoT devices, especially not through their entire lifecycle. Supply chain security issues are even more difficult to tackle because of the layered nature of IoT software stacks.

We offer a tool for automated zero-day discovery and lifelong CVE monitoring that allows security engineers to focus on more complex problems. By integrating our solution into the CI/CD pipeline and offering easy-to-understand dashboards, IoT security can be managed throughout the production funnel simply and efficiently.

HOW WE HELP



BUGPROVE

Save time and costs
Resource Utilization & Extensive Analysis

Manual security testing eats up engineering resources. **BugProve** saves you time to have a leaner and smoother security testing process.

BUGPROVE

HOW WE HELP

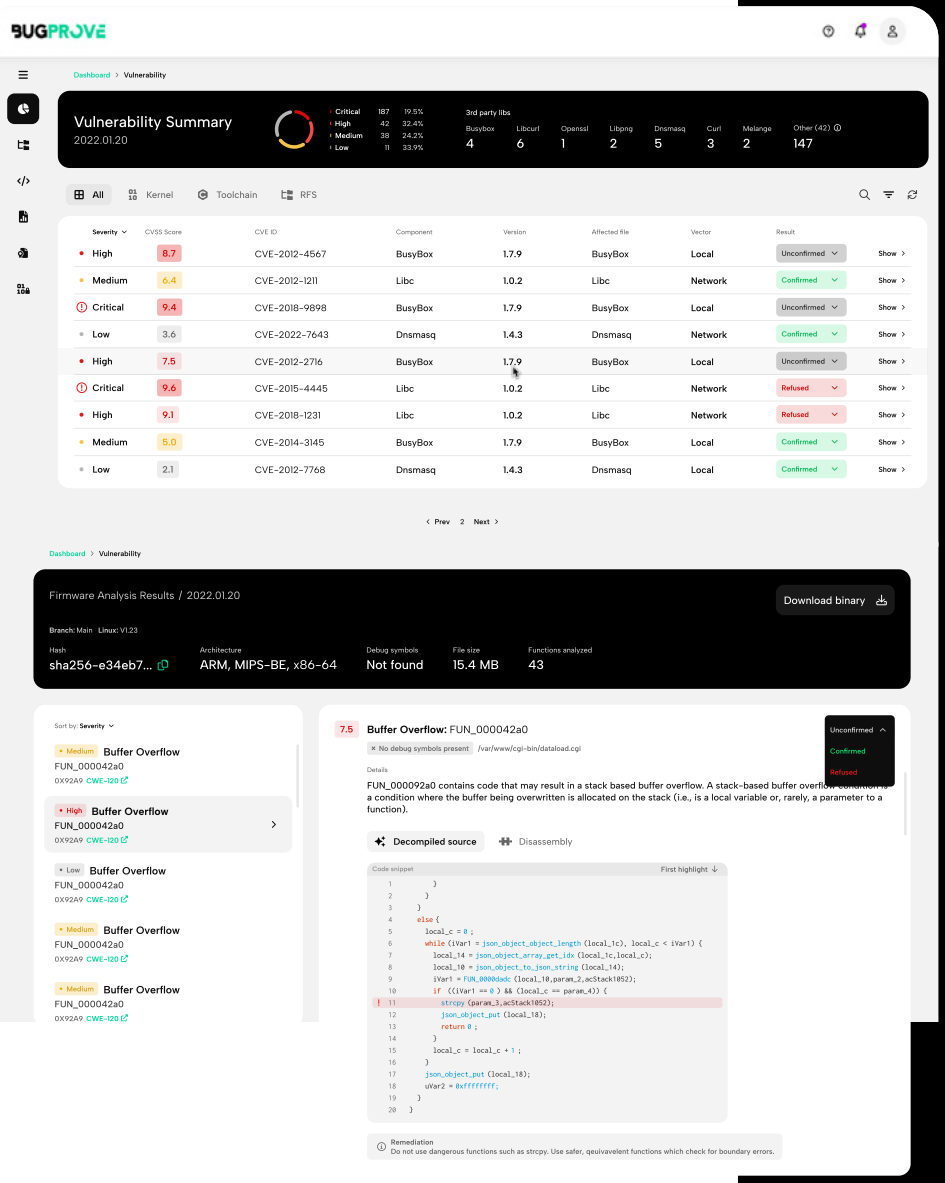
Our autonomous security testing saves you time and money as it automates the detection of critical vulnerabilities. We achieve this by pushing the boundaries of binary analysis with **integrated zero-day vulnerability discovery.** Our tool exposes security issues that are hidden in your third-party SDKs to help you decrease your supply chain security liability as well. **Catching known vulnerabilities (CVEs)** and other security issues present in the SDK of your firmware will help you to stand behind the security posture of your final product with confidence.

Integrating BugProve into your CI/CD process will support the work of any CISO or CTO. Our tool enables them to cut down on development costs by catching issues early and eliminating **testing downtimes taken up by security administrative tasks**, while our remediation recommendations help engineers to secure your firmware. Such improvements in security testing lead to a streamlined development process, increasing trust and confidence that there will be no unexpected show-stoppers before product releases.

Finally, our lifelong **continuous monitoring solution** will help your security posture stay robust as time goes on. It will ensure that you are up-to-date with upcoming security regulations and stay on top of your game.

TAKE CONTROL OF YOUR SECURITY WITH
BUGPROVE'S AUTOMATED FIRMWARE ANALYSIS

BUGPROVE



WHAT IS OUR SECRET?

UNIQUE PRODUCT CAPABILITIES

We analyze complete firmware binaries and support integrations with build pipelines based on popular tools like Buildroot and Yocto (OpenEmbedded). Our tool **can analyze entire embedded Linux firmware images, as well as individual ELF binaries,** mainstream embedded architectures like ARM, MIPS and x86-64

BugProve's scans provide an accurate, in-depth summary **of known CVEs** present in the components of your firmware. We also created a detailed dashboard to help you track these vulnerabilities at a glance and export **actionable reports** tailored to your needs. User-friendly UI makes navigating our tool a breeze, so you can stay focused on what matters the most: your product security.

PROVEN TRACK RECORD

Using BugProve, vulnerabilities have already been found in the products of:

- Silicon Labs
- Honeywell
- Netgear
- Broadcom
- Asus

All our scans run on firmware images and binaries, no source code is required:

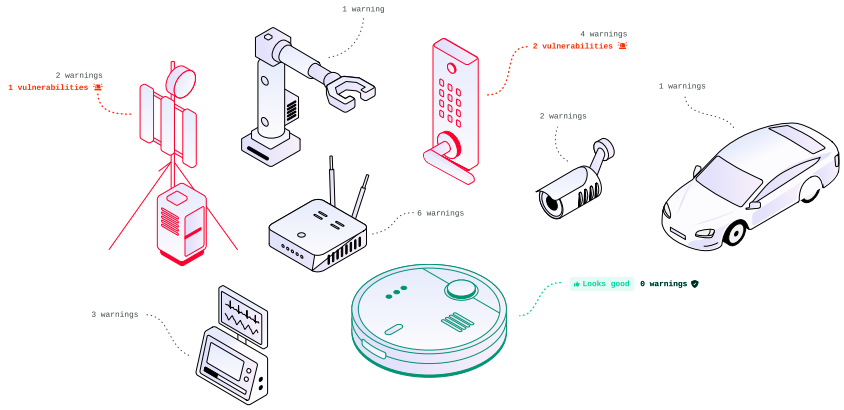
- advanced static and semi-dynamic analysis
- unique multi-binary taint analysis
- cryptographic analysis
- hardening and security configuration checks
- vulnerability **remediation**

BUGPROVE

OUR STORY

Founded in 2022, our mission is to restore stakeholder trust in embedded systems by helping IoT device manufacturers minimize security risks and improve their security posture.

The idea of BugProve dates back to the mid-2010s when the three of us worked together on embedded system security testing. It quickly became clear that the IoT sector was facing monumental challenges caused by the growing number of device vulnerabilities and malicious activities. This led us to create an automated solution to address various IoT security issues in the early stages of development, well before embedded devices are released to the market.



Eventually, Credo Ventures and Fiedler Capital – both prestigious CEE investment firms with a great track record – saw the potential in the idea. They provided the seed investment necessary to start the research and development activities in Budapest, Hungary.

We now have a dedicated team of 10+ experts with plans to expand to keep up with the growing interest surrounding our product.

LEVEL UP YOUR IOT SECURITY!

BugProve

sales@bugprove.com

https://bugprove.com/