Pentesting of Cellular IoT Devices.

Protect your product and your reputation.

www.tuv.com/pentest

TÜVRheinland®
Precisely Right.

OUR SERVICE

- By using a well structed testing approach, we test your cellular IoT device for security vulnerabilities that a hacker could exploit.
- Overview of the weaknesses that may affect the security of your cellular device.
- Recommendation for improving the security of your cellular device.
- In addition to the next standard communication channels, our test also includes 2G/3G/4G and in the near future also 5G connections.

YOUR ADVANTAGES

- By using automated as well as manual tests we provide insight for known and unknown weaknesses in your product.
- You understand the attack surface and weaknesses in your product to provide a more secure and more reliable product.
- You learn about weaknesses in your product before a hacker can exploit them. This gives you time to remediate weakness and helps you to protect the reputation of your brand.
- Our report provides information for executives as well as system engineers.
- Overall our service supports you in building and operating a more secure ginez device, protecting your data and your reputation.

OUR COMPETENCE

- Over 20 years experience in penetration testing.
- Every year, we carry out more than 1,000 penetration tests and IT security analyses all over the world.
- Our security testers concentrate on penetration testing. In addition, they hold well-recognized industry certificates, e.g., OSCP, OSCE. Overall, this ensures high quality of the results.
- Development laboratory for compliant testing and own test systems for long range (2G bis 5G) and for short range (Wi-Fi, BT, BT-SIG, LoRa and so on).

OUR METHODOLGY

1. KICK-OFF AND SETUP

We start our project with a kick-off in which we define the exact scope of the project, present the prerequisites of the analysis to ensure good results, and discuss the proper setup of the analysis.

2. SETUP AND BASIC FUNCTIONALITY TEST

We setup the device in our lab and check if it works as expected by doing some basic functionality tests before starting the analysis.

3. INFORMATION GATHERING

We start your analysis with an information gathering phase. In this phase, we collect various pieces of information about the system and its typical operational environment. This helps us to understand the product and the attack surface of the product.

4. IDENTIFICATION OF VULNERABILITIES

In this step, we start to search for potential vulnerabilities and weaknesses. This includes known vulnerabilities through automated scans and unknown vulnerabilities through manual tests.

5. EXPLOITATION OF VULNERABILITIES

Once we have identified potential vulnerabilities, we start to exploit them. This aims at sorting out false-positives and understanding the risks that come with the vulnerability. In addition, it provides more insights on the product.

6. REPORTING

In the next step, we document our results in a TÜV Rheinland report. The report includes a management summary as well as detailed information on the vulnerabilities found. It includes also recommendations on remediation strategies for fixing the vulnerabilities.

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Cologne, Germany
pen_cellular_testing@tuv.com
www.tuv.com/pentest

TÜVRheinland®
Precisely Right.