CyberDanube:

Food and Beverage Appliance Pentesting

In-Depth Technical Security Assessment of Food and Beverage Appliances

In today's fast-paced world, smart food and beverage equipment (industrial dishwashers, refrigerators, etc.) are an essential part of the warehouse industry. They drive efficiencies in inventory management and enhance the customer experience. This allows retailers to adapt to changing consumer preferences for convenience and quality.

Despite the rise of smart food and beverage devices in warehouse, security is often an afterthought. A malicious actor could exploit these connected devices to disrupt the supply chain, causing problems such as product shortages or oversupply. As technology advances, it's critical for any kind and size of store to prioritize security measures to protect their operations and ensure customer trust.

Preparations

- Kick-off Appointment
- Precise scoping definition

The assessment begins with a scope definition during a kick-off meeting. During this meeting, assessment priorities are set and security questions, such as „Is the device vulnerable to network-based attacks?“ or „Are backdoors installed on the device?“, are asked. Existing documentation and information about communication with public endpoints is shared to ensure an efficient process.

Technical Assessment

- Analysis of the software stack
- Testing means of communication
- Checking for holes in the Firewall

The technical assessment always begins with reconnaissance. What software is in use? What are the means of communication? What is being communicated? Many such questions are answered and compiled into an attack matrix, a list of possible weaknesses. This matrix serves as a roadmap for identifying vulnerabilities that could be exploited by malicious actors. By analyzing the information gathered, our security team can prioritize its efforts and focus on the most critical areas that require immediate attention.

Typical Challenges

- Limited documentation
- No source-code
- No or limited console access to the device

Device communication protocols are often proprietary or custom written with little to no documentation. This makes testing much more difficult because before it is even possible, the protocol must be reverse engineered. In fact, this can be the most difficult part. Access to source-code of the protocol or service implementation is also very rare to be provided. In combination with limited console access to the device, a lot of challenges can be present during such a pentest.

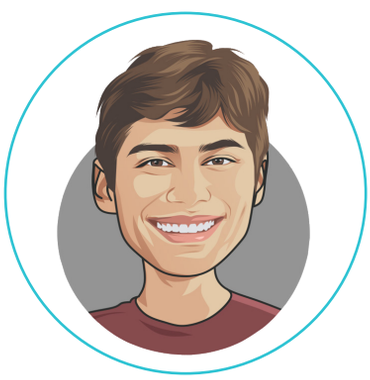
Common Vulnerabilities

- Broken Access Control
- Cryptographic Failures
- Injection
- Identification and Authentication Failures
- Denial of Service
- Security Logging and Monitoring Failures

We often identify several critical vulnerabilities in food and beverage equipment. From Denial of Service vulnerabilities that allow us to reboot or completely shut down the device, to taking full control of the device. Some require physical access to the device and some are completely remote.

Many security breaches can be prevented with proper testing. If you want to mitigate problems before they occur, contact us at office@cyberdanube.com.

Experts Contact



David Blagojevic
Industrial Security Expert

About CyberDanube

CyberDanube is a specialized cyber security company, offering OT, (I)IoT & Embedded Security testing services. CyberDanube provides a unique security toolset & technical consulting, e.g. penetration testing capability with a dedicated hardware lab for in-depth product analysis. With a proven track record in pentesting, research and published advisories including zero-day vulnerabilities, CyberDanube is a trusted authority (CNA) which operates independently from manufactures & investors as trustworthy partner in the security industry.

If you need a Pentest of a OT Infrastructure or an (I)IoT/Embedded Device,

Contact us via : office@cyberdanube.com

This Whitepaper has been inspired by real word projects.