VDOO

Whistler™

Real-Time IoT Threats Feed

DATASHEET

The Use of Third-Party Software in IoT Devices

Smart connected devices are becoming more and more common, surrounding us in our day to day lives. Unfortunately, many of these devices have not implemented basic security building blocks, opening the door to emerging risks and attacks. Smart devices are highly dependent on third party software, including many different open source components. While this allows flexibility, lower costs, and customization capabilities, it also creates dependency on rapidly changing, and in many cases insecure, code that is accessible to adversaries, or on stagnant code that its developer community is no longer engaged in improving so it lacks new patches. Because of its inherent flexibility and widespread usage, open source related vulnerabilities are an easy, efficient, and effective target for hackers.

IoT Manufacturers Inherent Challenge

Using third party components can be extremely helpful and reduce development time and costs; however, it creates a major challenge for manufacturers to continuously be aware of new security vulnerabilities discovered in third party or open source code and act accordingly. Due to the variety and the rapid changes in open source software, manufacturers might also be, knowingly or unknowingly, using abandoned software. In such software components, vulnerabilities are much more likely to be identified by adversaries and not by the developer community, making it hard to learn about new vulnerabilities, and making it virtually impossible to fix issues found.

IoT Device Operators Can’t Be Left Behind

Enterprise IoT devices, regardless of the device type or location of use, suffer from the aforementioned issues of using third party software, frequent vulnerabilities, lack of visibility, and dependence on the developer community. As opposed to IT applications where IT administrators and security teams have visibility and control over third party software introduced to their networks, when adding an IoT device, the IoT device operator has very little visibility and knowledge about the specific software packages introduced to his network. In order to keep their devices and networks secure, IoT device operators must constantly be aware of security risks and vulnerabilities discovered in their devices.

Stay Secure with Up-To-Date Threat Intelligence

Vision™, VDOO's automated analysis solution, automatically breaks down every device's firmware to its most specific components—both hardware and software. VDOO continuously scans all firmware binaries and queries its own and all other known vulnerabilities databases to find new device threats. This allows VDOO to determine the risks and vulnerabilities the device is exposed to. Whistler™ provides ongoing visibility to newly found device security gaps and points to suggested remediation steps. It can bridge a major gap for both device manufacturers or users, as both need visibility into the packages that exist on the device, and the knowhow to fix or mitigate new issues on the device, as close as possible to real-time.

About VDOO

VDOO was established in 2017 to pioneer embedded systems security, with an end-to-end solution of security automation, certification, and protection. The VDOO founders' backgrounds include an endpoint cybersecurity startup acquired by Palo Alto Networks, as well as notable experience serving in the Israeli Intelligence Elite Unit. For additional information, please contact us at info@vdoo.com or visit our website at vdoo.com.

VDOO

Key Features

- Real-time alerts feed
- Device focused new vulnerabilities
- Step-by-step mitigation guide

Key Benefits

✓

- Stay up-to-date with the latest security updates relevant to your IoT devices
- Mitigate threats as they emerge
- Take proactive measures to protect the device and network

Related Products

- VDOO Vision™
- VDOO ERA™
- VDOO Quicksand™