Dear Blickfeld Customer,
Blickfeld engineering has identified a security issue in the Percept Software, which may affect your use of the software. Please review the Security Advisory notice to determine if the issues apply to your environment.

BF00001
Exposed Docker Engine API port may allow local privilege escalation or Remote Code Execution

Summary
Blickfeld Percept uses the Docker Engine API to launch additional subcomponents as Docker containers. This requires making the Docker Engine API accessible from our main Docker container. The method we chose for this on Linux operating systems caused the Docker Engine API to bind to port 2375 on all network interfaces. On Windows operating systems it binds to port 2375 on the link local interface.

Due to the architecture of Docker, access to this port can enable remote or local attackers to execute code or escalate their privileges. In most typical installations, a firewall or router prevents direct access to this port, leaving only internal users on the same network or the same machine as potential attackers.

The updated Percept Version 1.4.1 removes the port-based communication and instead uses a file-based communication to launch the Docker subcomponents. This file-based approach prevents non-privileged users and remote attackers from accessing the Docker Engine API.

Affected Products
- Vulnerable products:
    - All Blickfeld Percept Versions below 1.4.1

- Product confirmed not vulnerable:
    - Blickfeld LiDAR devices are not affected by this vulnerability

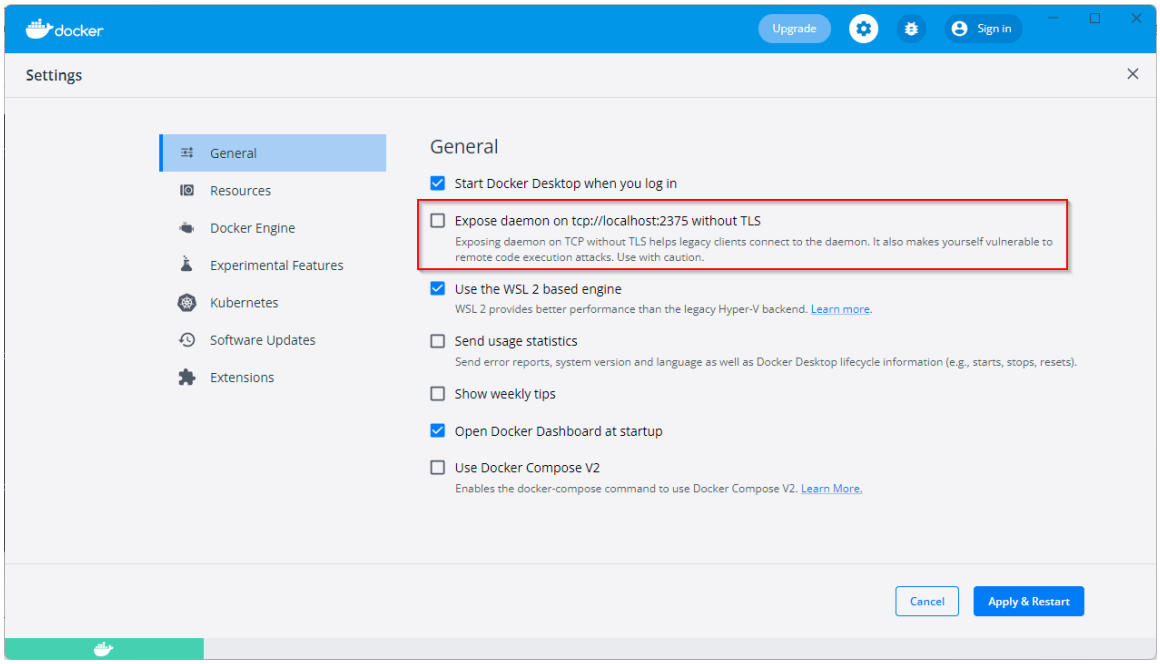
Affected Platforms
- Linux (Remote Code Execution, Local Privilege Escalation)
- Windows (Local Privilege Escalation)

Conditions
- You are using Percept before version 1.4.1
- An attacker has access to port 2375 on the device running Percept (local or, for Linux without Firewall, remotely)

Workarounds
- Protect port 2375 via firewall from network access (default behavior on Windows Systems, on Linux use e.g. ufw). Note that this can still allow Local Privilege Escalation. OR
- Disable the Docker Service until you can perform an upgrade (this renders Percept unusable)

Solution

- Linux Platform: Install Percept 1.4.1 or later and follow the steps for reverting the changes to Docker setup introduced by Percept 1.4.0 or older from this website: https://docs.blickfeld.com/percept/latest/percept-manual/v1.4.1/fix_docker_daemon.html .
- Windows Platform: Install Percept 1.4.1 or later and disable “Expose daemon on tcp://localhost:2375 without TLS” in the Docker Desktop Settings:



Additional Resources
https://docs.docker.com/engine/security/#docker-daemon-attack-surface

Contact
support@blickfeld.com

Author: Rolf Wojtech
Rev. 1.0 2022-05-11