

**ETC Cyber Security Lab**

**Pentest Report**

**Proprietary Statement**

© 2021 Trane Technologies, All rights reserved worldwide. No part or parts of this documentation may be reproduced, translated, stored in any electronic retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the copyright owner. Trane Technologies retains the exclusive title to all intellectual property rights relating to this documentation.

The information in this documentation is subject to change without notice and should not be construed as a commitment by Trane Technologies, makes no representations or warranties, express or implied, with respect to the documentation and shall not be liable for any damages, including any indirect, incidental, consequential damages (such as loss of profit, loss of use of assets, loss of business opportunity, loss of data or claims for or on behalf of user’s customers), that may be suffered by the user.

**Trane Technologies,**

IBC Knowledge Park, 8th Floor, Tower D, 4/1,

Bannerghatta Main Rd, Bhavani Nagar,

S.G. Palya, Bengaluru, Karnataka 560029.

Email: [Arvind.Chikmath@tranetechnologies.com](mailto:Arvind.Chikmath@tranetechnologies.com)

www.tranetechnologies.com

**Project Name: test**

**Software Rev:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IMPLICIT CONFIDENTIALITY AGREEMENT**  This report contains information considered critical and thus confidential by Trane Technologies. By reading it, the reader implicitly complies to the following:   * Neither this report nor any of its content may be shared by the reader to any third party unless he (or she) has been explicitly authorized to do so. * Neither this report nor any of its content may be modified by the reader unless he (or she) has been explicitly authorized to do so. * SPOC of project team to whom the report is distributed is responsible for safe custody/ distribution of report. | | | | | |
| **Version** | **Document status** | **Lead Pen-tester** | **Reviewer** | **Distributed to**  **(SPOC of project team)** | **Date** |
| 1.0 | Final Test | Madhuri  [Gurudev.Togurge@tranetechnologies.com](mailto:Gurudev.Togurge@tranetechnologies.com) | Prashantha Kumar  [Prashantha.Kumar@tranetechnologies.com](mailto:Prashantha.Kumar@tranetechnologies.com) | Tom Marquette [Tom.Marquette@tranetechnologies.com](mailto:Tom.Marquette@tranetechnologies.com)  Mziray, Judith [Judith.Mziray@tranetechnologies.com](mailto:Judith.Mziray@tranetechnologies.com) | 2024-04-04 |

**Table of contents**

[**Executive Summary** 5](#_Toc112671801)

[Scope: 5](#_Toc112671802)

[Out of Scope: 5](#_Toc112671803)

[Summary of Findings: 6](#_Toc112671804)

[Summary of Recommendation/ Remediation: 6](#_Toc112671805)

[**Attack Narrative** 7](#_Toc112671806)

[**Risk and Ratings** 8](#_Toc112671807)

[**Vulnerability Details and Mitigation** 9](#_Toc112671808)

[List of Vulnerabilities 9](#_Toc112671809)

[Vulnerability Details 10](#_Toc112671810)

[1. Denial of Service Attack through Websockets 10](#_Toc112671811)

[2. HTTP Clear text communication 10](#_Toc112671812)

[3. Sensitive information disclosure in web page 11](#_Toc112671813)

[4. Vulnerable Operating System 12](#_Toc112671814)

[5. FTP Plain text communication 13](#_Toc112671815)

[6. Missing Operating system hardening 13](#_Toc112671816)

[7. Non-essential command services are running 14](#_Toc112671817)

# **Executive Summary**

ETC Cyber Security Team was contracted by TK Team to conduct a penetration test on Jolt system in development phase, to determine its exposure to a targeted attack on **14th July 2022.** Product security team started penetration testing on release after receiving the necessary details and hardware on **1st Aug 2022**. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against Jolt system controller with the goals of:

* Identifying if a remote attacker could attack.
* Determining the impact of a security breach on:
  + Product Information Leakage
  + Kernel Security

Efforts were placed on the identification and exploitation of security weaknesses that could allow an attacker to gain unauthorized access to data or information. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-1151 with all tests and actions being conducted under controlled conditions.

Final report on release has been shared with the project team SPOC on **29th Aug 2022.**

## **Scope:**

1. Jolt System with IA3 Controller
2. Communication with USB over ethernet

## **Out of Scope:**

1. GPS/GSM communication

## **Summary of Findings:**

## **Summary of Recommendation/ Remediation:**

It is recommended to test the Jolt System with release firmware.

Recommendations been mentioned against the found vulnerabilities in subsequent sections. These recommendations are as per best industry practices, recommendations like OWASP testing guidelines, PTES Technical Guidelines. It is advised to recheck the found vulnerabilities against every component and apply mitigations throughout the application.

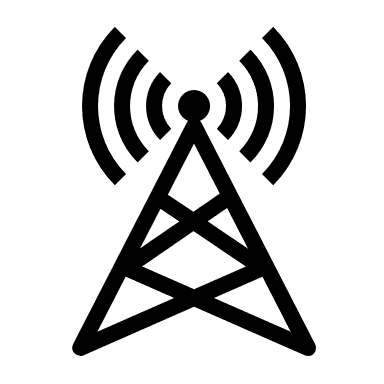
It is recommended to follow NIST guidelines. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>

# **Attack Narrative**

IA3 Controller

**Jolt**

**Pentest System**



USB over ethernet

GPS/GSM

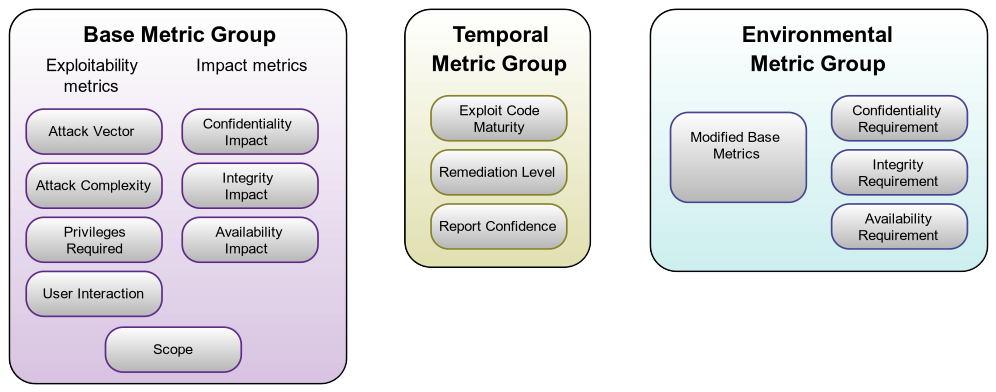
CAN

# **Risk and Ratings**

As per industry best practices, ETC Cyber Security Lab practices rating of vulnerabilities based on CVSS V3.0 (Common Vulnerability Scoring System). CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities.

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics.

The metrics are depicted below:



CVSS is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. The official CVSS documentation can be found at <https://www.first.org/cvss/>

Vulnerability Severity Ratings (CVSS 3.0):

|  |  |
| --- | --- |
| Severity | Base Score Range |
| None | 0.0 |
| Low | 0.1-3.9 |
| Medium | 4.0-6.9 |
| High | 7.0-8.9 |
| Critical | 9.0-10.0 |

For understanding the standards, follow the free self-paced online training course at <https://www.first.org/cvss/training>

# **Vulnerability Details and Mitigation**

## **List of Vulnerabilities**

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Vulnerability | Severity | Status |
| 1 | Denial of Service Attack through Websockets | Medium | Open |

## **Vulnerability Details**

## OTA Crypto key sniffing

**Rating:**

**CVSS:**

**Description:** Attackers intercept and decrypt cryptographic keys exchanged over-the-air during device updates.

**Impact:** Enables unauthorized access to encrypted data and compromises device security.

**Remediation:** Implement secure encryption protocols and mechanisms for OTA updates, such as using secure channels and strong encryption algorithms.

**Evidence:**



## RAM Dump Attack

**Rating:**

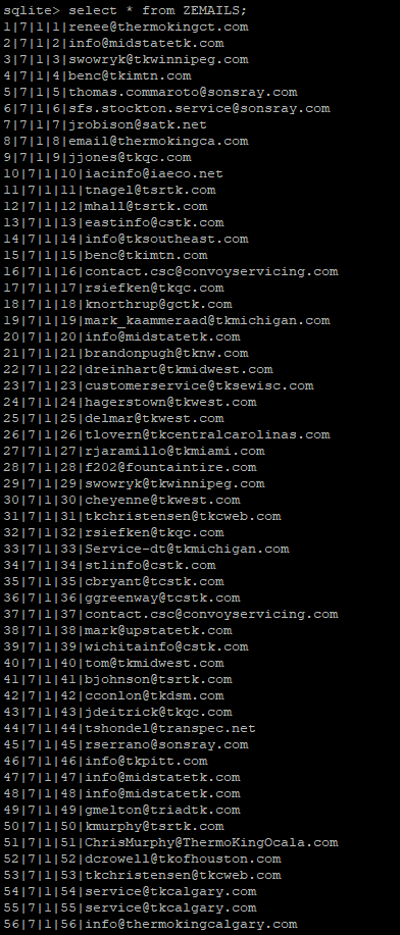
**CVSS:**

**Description:** Attackers exploit vulnerabilities to dump the contents of a device's RAM, potentially revealing sensitive data.

**Impact:** Allows attackers to access sensitive information stored in RAM, including encryption keys or user credentials.

**Remediation:** Employ secure coding practices, memory protection mechanisms, and encryption for sensitive data stored in RAM.

**Evidence:**



## lack of CRC verification

**Rating:**

**CVSS:**

**Description:** Data packets lack CRC verification, enabling transmission errors to go undetected or manipulated.

**Impact:** May result in data corruption, tampering, or injection attacks compromising the integrity of transmitted data.

**Remediation:** Implement CRC or checksum verification mechanisms to detect and reject corrupted or tampered data packets.

**Evidence:**

