September 29, 2023

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Rockwell Automation PanelView 800 vulnerability. The vulnerability affects PanelView 800 versions 2711R-T10T: V3.011, 2711R-T7T: V3.011 and 2711R-T4T: V3.011. Successful exploitation of this vulnerability could allow an attacker to disclose sensitive information, modify data, or cause a denial-of-service. This vulnerability potentially impacts the energy, water, wastewater and telecommunications sectors.

Technical Details

An input/output validation vulnerability exists in a third-party component that the PanelView™ 800 utilizes. Libpng, which is PNG's reference library, version 1.6.32 and earlier does not properly check the length of chunks against the user limit. Libpng versions prior to 1.6.32 are susceptible to a vulnerability which, when successfully exploited, could potentially lead to a disclosure of sensitive information, addition or modification of data, or a denial-of-service condition.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2017-12652
- ICSA-23-271-01 Rockwell Automation PanelView 800

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts