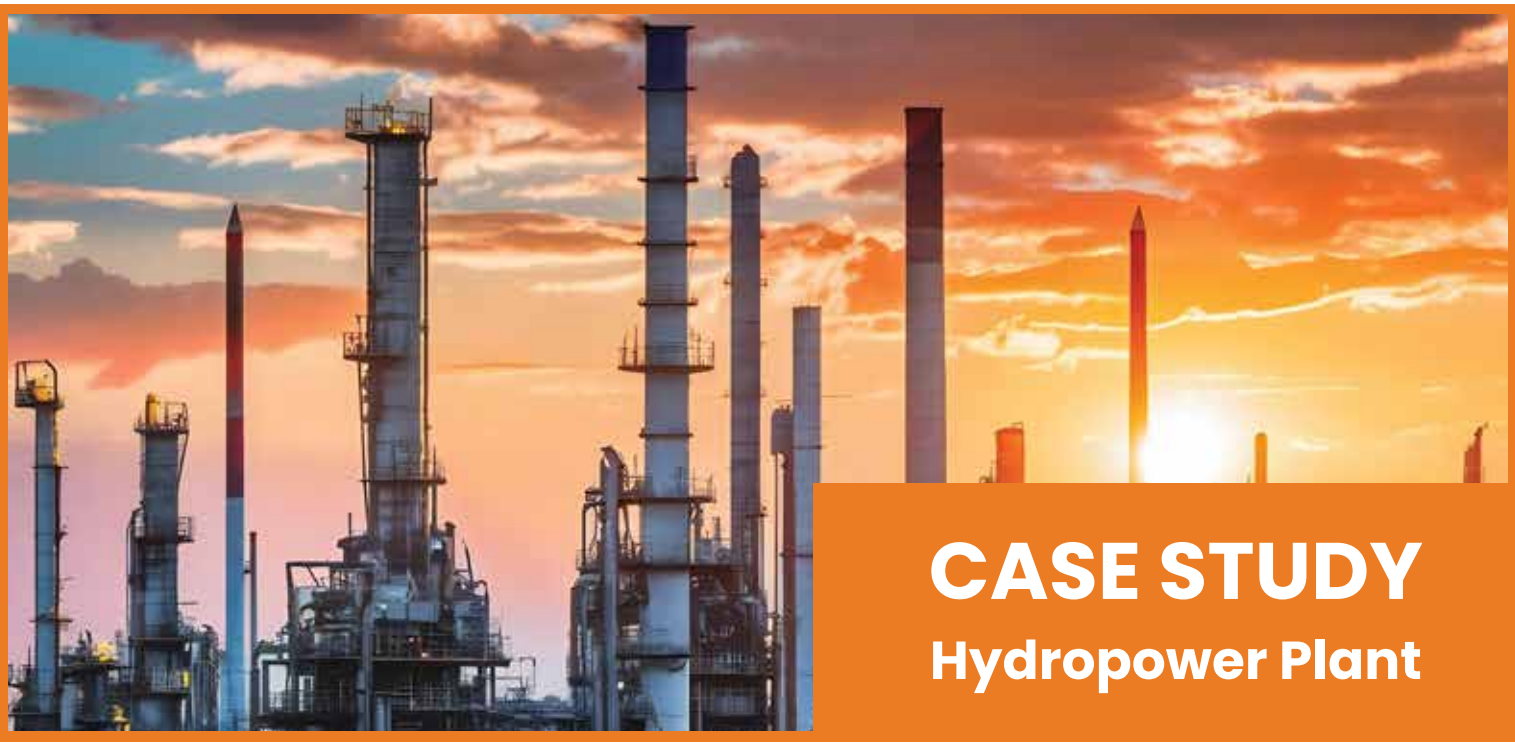
KRATIKAL
SECURE FOR SURE

www.kratikal.com



CASE STUDY

Hydropower Plant

Client Background

A prominent organization in India, renowned for harnessing the region's hydroelectric potential, operates plants ranging from 1.5 MW to 304 MW, with a total capacity of more than 1400 MW. It plays a crucial role in the energy sector. Known for its commitment to renewable energy. This entity significantly contributes to the state's economic growth and energy sustainability.

Business Challenges

- Cybersecurity threats
- Aging infrastructure
- Integration of renewable energy sources
- Regulatory compliance
- Operational continuity
- Supply chain security
- Data integrity and privacy
- Remote access and monitoring

Environment

- SCADA Interface
- Internal Network comprising Firewall
- Router, Sensors

Solution

The organization approached Kratikal's security testing department to identify bugs potentially causing service disruption or data leaks from insider attacks. They also sought guidance to mitigate risks arising from these vulnerabilities.

We found some serious vulnerabilities that can impact the entire organization, business loss, data leak, and unauthorized access.

Risk

- An attacker can do Remote Code Execution on the Apache Server
- Leakage of Sensitive Data (Username and Password) through MiTM attack, due to use of unsecured channels (HTTP)Unauthorized person can access the critical hardware, like Flow Sensor, to manipulate the Data and can cause serious harm to the DAM facility.
- Using default credentials can lead to severe risks such as unauthorized access, data breaches & information leak

Major Findings

- Lack of Security on communication channels
- Lack in physical Security for Accessing the critical hardware
- Use of Vulnerable and Outdated firmware in critical assets.
- Default credentials were used for authorization in some of the network devices.

Our Approach

- **Black Box Testing:** Conducted Black Box testing on all external-facing assets to identify external threats.
- **Configuration Audit:** An authenticated-based configuration audit approach is followed to identify vulnerabilities in the critical assets.
- **Communication Channels:** Analyze if data manipulation can be done and what can be the outcome of that on SCADA.
- **Provided Machines:** Tested specific machines provided by the organization.
- **Up-to-Date Pentesting:** Used OWASP's IoT top 10 standards.

Impact

- Using default credentials, configs can allow an unauthorized person to access, change, modify critical data.
- No authorization to access sensitive data, critical assets like sensors can lead to serious damage.
- Communication over insecure network or channel can lead to sensitive data leak

Recommendations

- Kratikal's security team provided an advisory to update the Server to the latest version.
- Use of Secure Communication Channels like HTTPS, WSS, and Other Secure Channels
- Adding More Physical Security for accessing sensitive hardware/sensors
- It is recommended to use strong passwords and rotate all the passwords within 90 Days.
- Updating all the outdated components of the application, and adding authentication to the admin panels.

Kratikal Privacy Commitment

Kratikal is dedicated to safeguarding your company from advanced threats, such as data leakage. For this reason, we do not reveal the names of our case study participants.

sales@kratikal.com

www.kratikal.com

+91-9289192210

5th Floor, A-5, Block A, Sector 68, Noida(UP) 201301