Abysmal State of Global Critical Infra Security:

Supply of Gas, Water, & Govt. Services at High Risk

Author: Sparsh Kulshrestha, Senior Security Analyst, CloudSEK

Editor: Deepanjli P, Lead Cyber Intelligence Editor, CloudSEK

CloudSEK

Contents

Rise in Cyber Attacks on Critical Infrastructure Systems

In the past year there has been a considerable increase in cyber attacks targeting critical infrastructure systems across the world, with a recent survey highlighting that over 90% of organizations that use operational technology (OT) systems have experienced some sort of cyber incident in the past year. These attacks have ranged from the malware induced power outage in Mumbai to the ransomware attack on the Colonial oil pipeline. More recently, a nation-state actor targeted the port of Houston by exploiting a zero-day in a Zoho user authentication device.

Owing to an increase in remote work and online businesses, most cybersecurity efforts have been focused on IT security. However, the recent OT attacks have been a timely reminder of why traditional industries and critical infrastructure need renewed attention, given that they form the bedrock of our societies and our economies.

OT Attacks Impact Governments, Businesses, and Individuals

Critical infrastructure systems or industrial control systems (ICS) are used by private and government entities to monitor or control processes in various industrial and manufacturing sectors. And the availability of the products and services provided by these sectors determine the stability and reliability of a country's economy.

Recent Cyber Attacks on Industrial Systems

Some of the recent attacks on critical infrastructure systems that have had far reaching impact include:

- **Ukrainian Power Outages**: In December 2015 a massive power outage hit Ukraine. It was found to be the result of a cyber attack on a supervisory control and data acquisition (SCADA) system. This instance left ~230,000 people in the west of the country without power for hours.
- **Rye Brook, New York Dam Attack**: In this instance a small dam in Rye Brook, New York became a national concern. The U.S. Justice Department claimed that it was as Iranian attack on U.S. infrastructure, in which hackers succeeded in accessing the core command-and-control system. And the nation state actors were able to carry out this using only a cellular modem.
- **SWIFT global bank messaging system**: Spanning 2015 and 2016, the SWIFT global messaging system, which is used by banks to move money around the world, was infiltrated by hackers from North Korea. Given that consistent banking transactions are key to an economy, this attack proved to be crippling. These attacks resulted in millions of dollars being stolen and were linked to a group called Lazarus, known for its ties to North Korea.

Can Anybody with Access to the Internet Target an ICS?

CloudSEK focuses on monitoring and analyzing the uncharted, yet rapidly evolving, external threat landscape. As part of our research on the overall security of OT systems, we set out to identify how easy or difficult it would be for threat actors to identify and infiltrate vulnerable critical infrastructure systems across the world. While nation state actors have an abundance of tools, time, and resources, other threat actors primarily rely on the internet to select targets and identify their vulnerabilities.

Identifying Vulnerable Critical Infrastructure Systems

While most ICSs have some level of cybersecurity measures in place, human error is one of the leading reasons due to which threat actors are still able to compromise them time and again. Some of the common weaknesses that threat actors, without the most sophisticated of tools and resources, look for in critical infrastructure systems are:

- Weak/ default/ obvious passwords
- Outdated versions of installed software
- Third-party vendor data leaks
- Common infrastructure vulnerabilities (SQLi, XSS, RCE, etc)
- Leaked Source Code on GitHub
- Shadow IT
- Phishing (Out of Scope for this research)

We began our research to scan for internet exposed critical infrastructure systems that have one or more of the above mentioned weaknesses. During the course of our research we identified hundreds of vulnerable ICSs. However, in this research paper we delve into 4 ICSs, across the private and government sectors, which are representative of common vulnerabilities and their impact on a nation's security and economy.

Note: This research follows the guidelines of CloudSEK's Responsible Disclosure Policy (Please check Appendix for complete details)

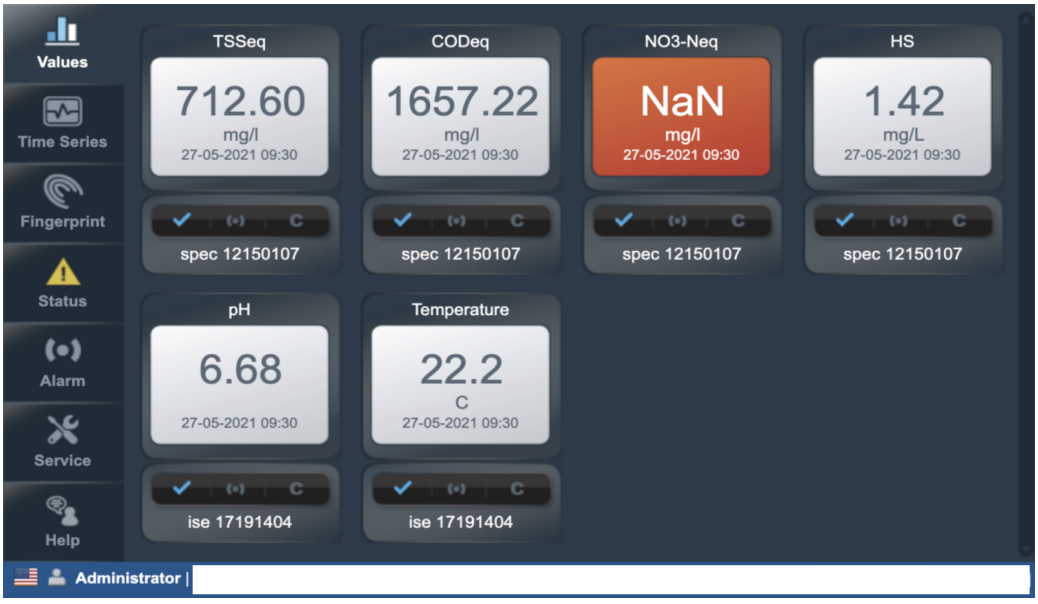
In-Depth Look at Some Vulnerable ICSs

The 4 examples that are representative of the extent and impact of cyber attacks on ICSs are:

1. Misconfigured instance of the water quality management software of an Indian conglomerate
2. Credentials of Government of India's Mail Server exposed on GitHub
3. Private gas transport company in India
4. Hard-Coded Credentials on Government of India's Central View Dashboard

1. Water Supply Critical Infrastructure Highly Prone to Cyber Attacks

Impacted Entity	Vulnerable System
s::can GmbH Online Water Quality Monitoring dashboard of an Indian FMCG company.	Exposed instance of a water quality management software.
Weakness	**Impact**
The tool was configured using default manufacturer credentials, enabling attackers to easily access the critical infrastructure of the water treatment plant.	Attackers can: • Edit/ modify water supply calibrations • Stop multiple pivotal operations that treat the water • Manipulate the chemical composition of the water



Admin dashboard of the water supply infrastructure

A wide-spread issue

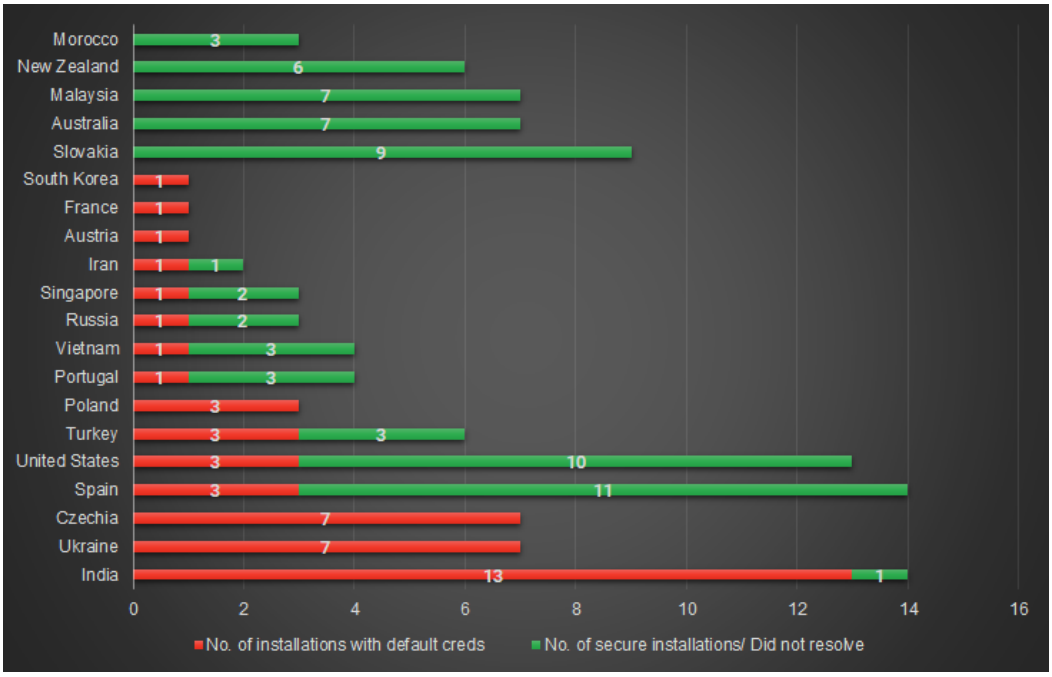
Global distribution of vulnerable water management software installations

Since the water quality management software is widely used by many of the popular water sources across the world, CloudSEK performed an internet-wide analysis of the misconfiguration.
Here is the global distribution of installations of the water quality management system that we discovered:

Country	No. of installations with default credentials	No. of Secure installations or Failed to resolve	No. of installations
India	13	1	**14**
Ukraine	7	0	**7**
Czechia	7	0	**7**
Spain	3	11	**14**
United States	3	10	**13**
Turkey	3	3	**6**
Poland	3	0	**3**
Portugal	1	3	**4**

Vietnam	1	3	**4**
Russia	1	2	**3**
Singapore	1	2	**3**
Iran	1	1	**2**
Austria	1	0	**1**
France	1	0	**1**
South Korea	1	0	**1**
Slovakia	0	9	**9**
Australia	0	7	**7**
Malaysia	0	7	**7**
New Zealand	0	6	**6**
Morocco	0	3	**3**
	47	**68**	**115**

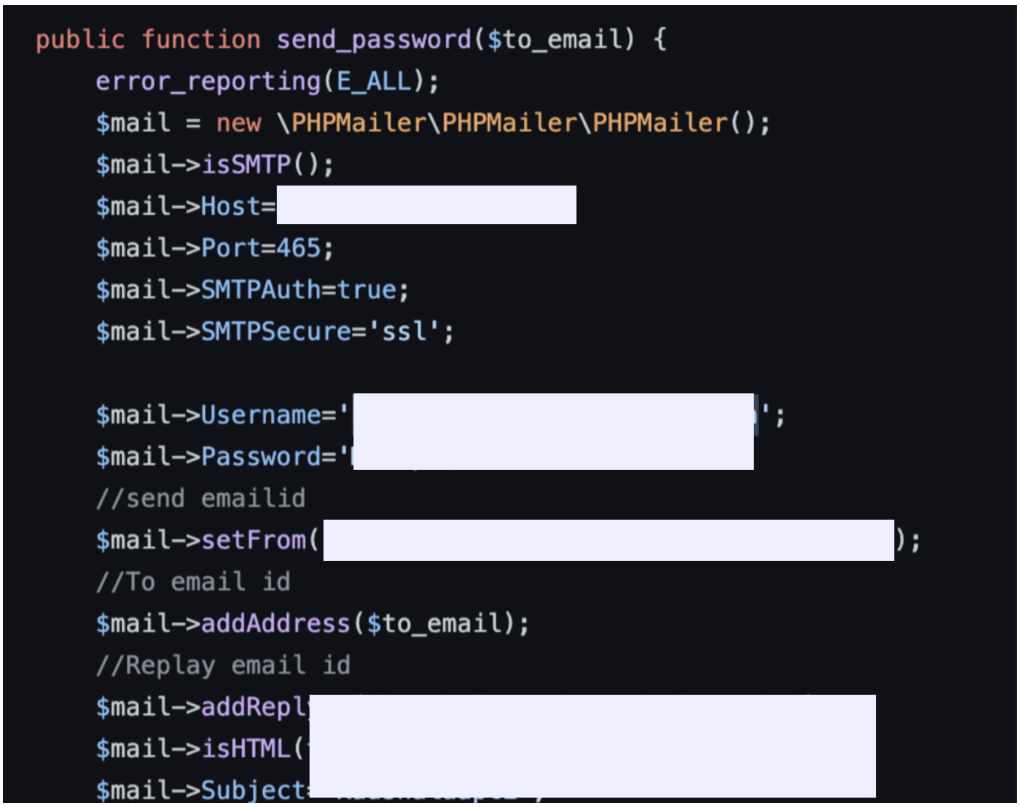
Of the 47 instances using default credentials, 30 of them belong to some of the major dams and water sources across the world, responsible for supplying drinking water to major cities across the globe. And India leads with 13 out of 14 installations having default credentials.



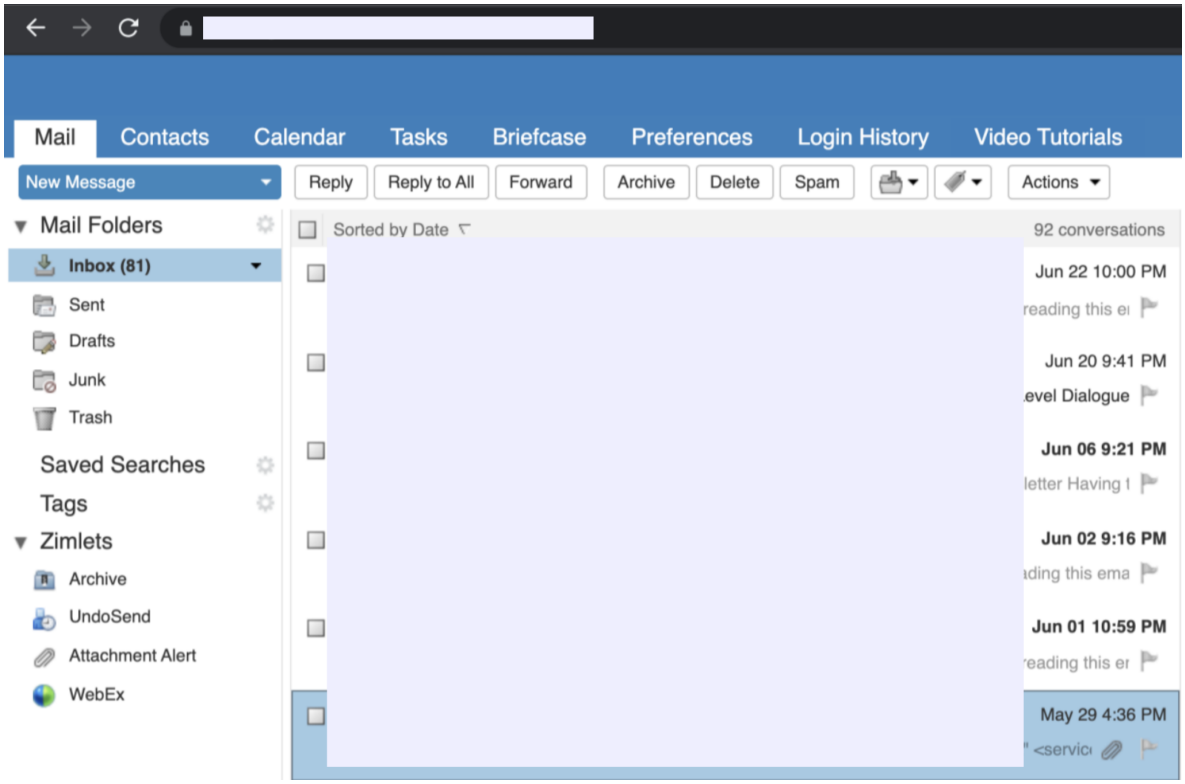
No. of installations with default creds vs secure/ inaccessible installations

2. Government of India's Mail Server Credentials Found on GitHub

Impacted Entity	Vulnerable System
Government of India	GitHub repository leaking mail server credentials. which contains credentials to the Indian government's mail server. hard-coded in the source code.
Weakness	**Impact**
The GitHub repository contains the credentials to the Indian government's mail server, hard-coded in the source code.	Attackers can: • Use access to the government email server to send emails impersonating trusted government entities and carry out social engineering campaigns. • They can also use it to spread misinformation. • Receiving a phishing email from a government email address will lure victims to more easily share their PII or click on suspicious links.



Government email server credentials hard-coded in the source code on GitHub



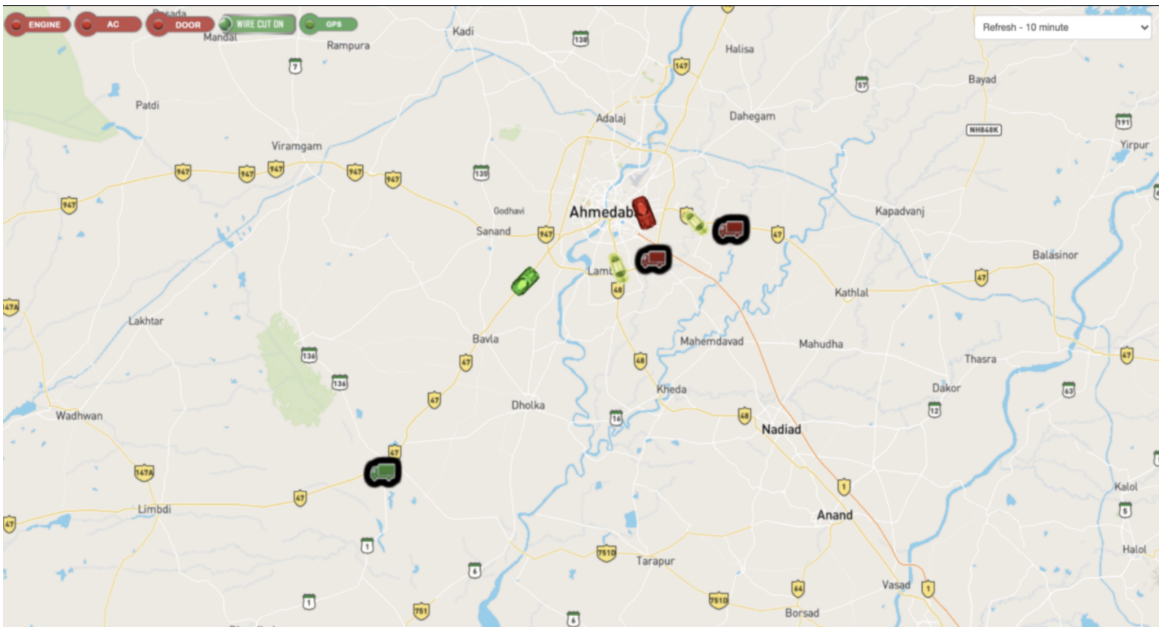
Email server can be accessed using the hard-coded credentials

Government entities procure a variety of goods and services, including software development and maintenance activities, from third-party vendors through the process of tendering. Many of these bidders are small software development companies that don't have stringent cyber security and monitoring strategies in place.

Given that multiple vendors have access to government networks and applications, it increases the chances of important data or credentials being exposed through unsecured S3 buckets and GitHub repositories.

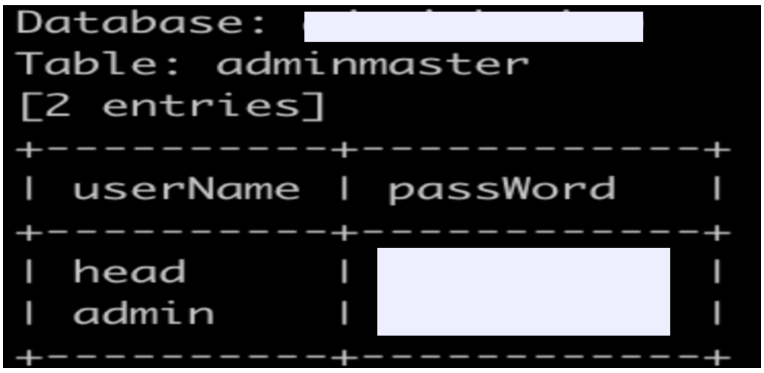
3. Gas Transport Truck Control Panel Vulnerable to SQL Injection

Impacted Entity	Vulnerable System
Gas Transport Company in India	XVigil monitors identified a web server that was the control panel for monitoring and managing Gas Transport Trucks.
Weakness	**Impact**
• The web server was hosting a default server page. • We then discovered the "/manager.jsp" endpoint via path enumeration which displayed the admin login page for the control panel. • This login page was found vulnerable to Blind SQL injection. • On successful exploitation, we observed the admin credentials were stored in plain text.	• The authenticated dashboard contained a lot of sensitive information about the trucks and it's drivers. • This includes the exact location of trucks (via GPS), licence plate numbers, drivers' phone number, and more. • Since these are not the regular trucks but the Gas Trucks, weaponizing this information could have disastrous consequences on public safety.



Real-time tracking of gas trucks

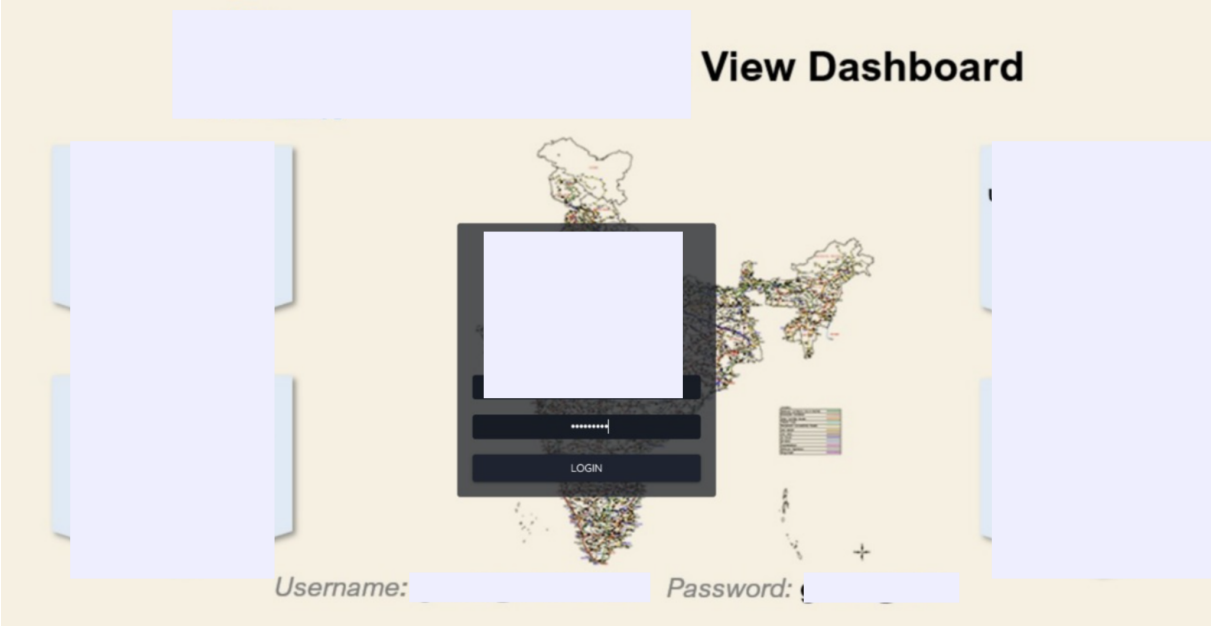
This again emphasizes the lack of security measures taken by the development firm. Apart from storing plaintext credentials, the only login page on the web server was vulnerable to SQL injection. Also, the credentials were so weak that they could have been guessed or brute-forced even if the login page was not vulnerable to SQL injection. These lapses indicate that the application hasn't undergone basic security testing.



Admin credentials stored in plaintext

4. Hard-Coded Credentials on Central View Dashboard

Impacted Entity	Vulnerable System
Government of India Central View Dashboard	A web server that hosts the central view dashboard for a nationwide critical infrastructure service. lets you monitor the CCTV footage of some services (which we do not wish to disclose) across all states in real-time.
Weakness	**Impact**
The credentials were hard-coded on the homepage of the application.	• Since the dashboard monitors in real-time, the CCTV footage of critical services, across all the Indian states, attackers can exploit it to surveil their targets. • The dashboard can also be used as an entry point and provide initial access to the network and enable further lateral movement.



Credentials of the central view dashboard hard-coded on the homepage

It is often assumed that if an application is hosted on a particular IP address and no DNS records are configured, it is secure. However, this does not hold true any more, given the availability of tools and techniques which index all IP addresses connected to the internet. So, it only takes a few clicks to go from an IP address to an organization's critical infrastructure.

Conclusion

With businesses, transactions, and interactions going online, governments and organizations are focusing on bolstering user privacy and IT security. However, this should also address the need for greater OT security. Given that critical infrastructure systems are the backbone of governments and large businesses, its overall security cannot be taken for granted.

Since gas, water, and government services are basic needs of a society, there needs to be a concerted effort to renew the emphasis on OT security. Apart from increasing awareness, we can also improve OT security by ensuring real-time monitoring of:

- Internet exposed OT applications
- Leaked credentials across GitHub and other repositories
- Underground forums for threat actors targeting OT systems
- Patches and work-arounds for vulnerabilities
- Unsecured cloud storage

Appendix

CloudSEK's Responsible Disclosure Policy

- We Ensure that we do not cause any damage while the detected vulnerability is being investigated. Our investigation must not, in any event, lead to an interruption of services or lead to any details being made public of either the asset manager or its clients.
- We do not place a backdoor in an information system in order to then demonstrate the vulnerability, as this can lead to further damage and involves unnecessary security risks.
- We do not edit or delete any data from the system and do not introduce any system changes.
- We do not try to repeatedly access the system and do not share the access obtained with others.
- We do not perform physical testing on any vulnerable devices that we identify.
- All the vulnerabilities found during this research were reported to the respective countries' CERTs (Cyber Emergency Response Team) via proper channels. We also provided significant time for them to respond to these findings before publishing this paper.

About CloudSEK

CloudSEK is an AI-driven Digital Risk Management Enterprise. CloudSEK's XVigil platform helps clients assess their security posture in real-time from the perspective of an attacker. XVigil scours thousands of sources (across the surface, deep and dark web), to detect cyber threats, data leaks, brand threats, identity thefts, etc. To learn more about how the CloudSEK XVigil platform can strengthen your external security posture and deliver value from Day 1, visit https://cloudsek.com/ or drop a note to sales@cloudsek.com.