Cyber Threat Advisory

30th June 2026

TLP:CLEAR

Critical Infrastructure Advisory

This advisory is relevant to all Samoan individuals, businesses and organisations that deal with critical infrastructure. This alert is intended to be understood by both general and technical audiences. Individuals and organisations that are involved in critical infrastructure are encouraged to remain vigilant and aware of cyber threats, and to apply available mitigations as soon as possible.

What's Happened?

Over the last few years, SamCERT has observed multiple threat actors increasingly exploiting access control vulnerabilities in Critical Infrastructure around the world.

Most notably, in December 2023, Iranian affiliated Cyber Actors systematically identified and exploited Programmable Logic Controllers in US Critical Infrastructure, including in US Water and Wastewater Systems Facilities. These threat actors exploited the following vulnerabilities:

- Weak default or non-existent passwords
- Inadequate Network Segmentation
- Internet-Exposed PLC Management Interfaces
- Lack of Multi-Factor Authentication

These threat actors leveraged these vulnerabilities to cause operational disruptions. Affected PLCs, devices and software had to be manually reset, incurring a financial and workload cost on the operating organisations.

While there were no major disruptions for the communities impacted, a similar attack in the future has the potential to cause significant cyber and digital harm.

What can we learn from this?

Whilst this attack against critical infrastructure did not happen in Samoa, there is the opportunity to learn from this event to better protect Samoan critical infrastructure and the communities they serve.

Threat Mitigations

Mitigating Controls: *Reduce the likelihood of your critical infrastructure systems being breached:*

1. Use passwords on all devices and accounts, ensuring that these passwords are distinct, complex, and long.
2. Implement Multi-Factor Authentication (MFA) on all devices and accounts, especially those that manage or control critical infrastructure.
3. Ensure that important hardware and interfaces are not internet-exposed. Change default ports and airgap critical systems away from public access.
4. Segment networks to increase resilience. Separate important networks through the use of firewalls and other measures of authentication to protect critical assets.

*a more detailed appendix is on page 2

Where can I go for help?

If you have been impacted information stealer malware, we encourage you to submit a report at:

www.samcert.gov.ws/report-incident

If you require more information, please contact SamCERT on:

samcert@mcit.gov.ws

+685 26 117

Cyber Threat Advisory

30th June 2026

TLP:CLEAR

Critical Infrastructure Advisory – Detailed Mitigations Appendix

This appendix intends to provide a more in-depth explanation of the threat mitigations mentioned on page 1. Introducing mitigations for access management and network security vulnerabilities is critical because these weakness are directly tied to who (or what) can access and control systems. In the case of critical infrastructure, that access often translates into real-world operational impact for the communities that rely on these critical infrastructure systems. Below are access management and network security-based control mitigations that can be implemented to strengthen critical infrastructure systems against common attack vectors. Detection is also important because it helps critical infrastructure quickly identify and respond to active threats before they cause serious damage or disruption.

Access Management

Access management controls are crucial for ensuring that only authorised applications, processes and users can execute actions within a system. Unrestricted software access and execution poses significant risk and an opportunity for adversaries to access functions and data that should be off limits. Mitigations in this area are:

Strong Passwords. These are passwords or passphrases that are at least 8 characters long and contain at least 1 uppercase letter, 1 lowercase letter, 1 number and 1 symbol. Strong passwords prevent adversaries from easily gaining access to critical systems.

Multi-Factor Authentication. Extra factors of authentication, beyond passwords, include one-time-passwords (through authenticator apps, emails etc), biometrics, hardware tokens and more.. Requiring users to provide more than 1 way of authentication significantly strengthens user authentication measures further reducing the likelihood of adversaries gaining access to a system.

Network Security

Network security controls are essential for protecting organisational resources from unauthorised access and ensuring that only trusted users and devices can connect to crucial systems. Unrestricted network access can pose significant risk and an opportunity for adversaries to access functions and control systems that should be off limits. Mitigations in this area are:

Network Device Hardening. Disabling unused ports, changing default ports, and preventing unneeded ports from being open to the internet reduced the number of exposed entry points that adversaries can exploit. Thus, reducing the attack surface and better protecting critical systems.

Network Segmentation. The practice of dividing a network into smaller, isolated segments ensures that systems and users can only communicate when necessary. This limits the ability of adversaries to move laterally across the environment and prevents a single compromise from impacting critical systems.

Reducing Attack Surface. Minimising the number of exposed services, interfaces, and entry points across systems reduces opportunities for adversaries to gain initial access. This includes removing unused software, disabling unused features, restricting external connectivity, and tightening access control pathways.

Detection

Detection Through Monitoring. Continuous monitoring of systems, networks, and user activities enables critical infrastructure to identity suspicious behaviour and potential security incidents in real time. By collecting and analysing logs, network traffic, and system events, security teams can detect anomalies and act according in a timely manner.