Waterstons
we're with you

+44 345 094 0945
www.waterstons.com

News article

Dec 2023

Cyber Incident Review

Hackers breach US water facility via internet exposed PLCs. Read about it here & what your organisation should do to stay protected.

State sponsored threat actors have breached multiple water treatment facilities in the USA via an internet exposed Programmable Logic Controller (PLC).

What Happened?

The US Cybersecurity & Infrastructure Security Agency (CISA) has confirmed that state sponsored threat actors breached multiple, unnamed water treatment facilities in late November. Following the attacks, CISA has attributed the attacks to threat actors affiliated with the Iranian Government Islamic Revolutionary Guard Corps (IRGC).

The threat actors who carried out the attack have claimed they targeted the organisations due to the use of equipment manufactured in Israel, specifically Unitronics Vision Series PLCs. The water treatment facilities that were breached had the Unitronics Vision Series PLC's publicly accessible via the internet. The PLCs were also using the default password – '1111' – and did not have any form of multi-factor authentication (MFA), or conditional access control enabled for remote access.

Once the breach was identified, the water companies were quick to respond and deploy incident response and business continuity plans, taking the impacted systems offline and switching to manual operations. The facilities have confirmed that there was no known threat to the water supply because of the attacks.

Wider Implications

This incident highlights the significant risk of a lack of secure configuration standards for IT and Operational Technology (OT) devices when deploying them in an organisation's network. Default passwords offer threat actors easy access to key systems and, despite the significant risk, are still frequently used.

In August 2023 accounts of LogicMonitor customers were breached due to customers not changing default passwords, with CISA identifying the use of default configuration of software and hardware as the top security misconfiguration in a recent report. While ultimately it is the organisation's responsibility to ensure default passwords and conditional access controls are in place, security researchers have encouraged manufacturers to adopt the requirement for default passwords to be changed on first sign in as a standard security measure. This incident also highlights the wider risk of state sponsored threats to organisations.

Over the past year, multiple government cyber security agencies including the UK National Cyber Security Centre (NCSC), FBI, and Australian Cyber Security Centre (ACSC) have warned of the growing state sponsored cyber threat to organisations, driven by the RussiaUkraine war. Now, as evidenced by the motivation for this recent attack, the recent Israel-Hamas conflict is igniting new state sponsored attacks.

Organisations Should

• Examine their own risk profile to determine if they are at a higher risk of attack from statealigned threat actors. Critical National Infrastructure (CNI) organisations and their supply chains, organisations affiliated with government, and culturally symbolic institutions will likely be the primary target of these attacks. However, all organisations should remain vigilant during this current period of heightened state-aligned cyber threats.

• Ensure that they develop and implement secure configuration standards for new devices requiring default password to be reset when new devices/applications are deployed in the either the IT or OT environments. Where appropriate, organisations should align with industry standard benchmarks such as the Centre for Internet Security (CIS) benchmarks.

• Review if remote access to the OT environment is required. If it is, ensure that all remote access is done securely via a VPN which requires MFA for login.

• Implement MFA for all accounts in both the IT and OT environment where appropriate. Where this cannot be deployed in the OT environment compensating controls should be considered.

• Ensure they have developed an incident response plan which is regularly tested and reviewed to ensure it is understood by key stakeholders in the organisation.

• Ensure they have implemented a comprehensive, well-tested and regularly reviewed business continuity plan to help minimise the impact of a cyber attack on business operations.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats.

We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430