Exploitation of Unitronics Programmable Logic Controllers (PLCs)

Alert status
High

Content complexity
Moderate

First published: 05 Dec 2023

Last updated: 05 Dec 2023

Content written for

- Small & medium business
- Large organisations & infrastructure
- Government

This Alert is relevant to Australians who use Unitronics PLCs in their environments which may not have applied appropriate cybersecurity practices and have the devices exposed to the internet.

Background / What has happened?

- Threat actors appear to be targeting Unitronics Vision Series PLCs since 22 November.
- Threat actors have likely used default-passwords to gain access to potentially critical systems and perform defacement, although the access they have obtained enables them to reconfigure the device.
- This example continues to highlight the risk of Internet-exposed Industrial Control Systems (ICS) and the access to potentially sensitive and critical systems they can provide.
- Additional Information can be found in advisories published by our partners:
    - IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities | CISA
    - NCSC statement following exploitation of Unitronics programmable logic controllers
    - Exploitation of Unitronics programmable logic controllers - Canadian Centre for Cyber Security

Mitigation / How do I stay secure?

These mitigations apply to all internet-facing PLCs, not just Unitronics.

Immediate steps to prevent attack:

- Change all default passwords on PLCs and HMIs and use a strong password. Ensure the Unitronics PLC default password is not in use.
- Disconnect the PLC from the public-facing internet or filter access to known internet endpoints that require access.

Follow-on steps to strengthen your security posture:

- Implement multifactor authentication for access to the operational technology (OT) network whenever applicable.
- If you require remote access, implement a firewall and/or virtual private network (VPN) in front of the PLC to control network access. A VPN or gateway device can enable multifactor authentication for remote access even if the PLC does not support multifactor authentication.
- Create strong backups of the logic and configurations of PLCs to enable fast recovery. Familiarise yourself with factory resets and backup deployment as preparation in the event of ransomware activity.

- Confirm third-party vendors are applying the above-recommended countermeasures to mitigate exposure of these devices and all installed equipment.

Assistance / Where can I go for help?

Organisations or individuals that have been impacted or require assistance can contact us via 1300 CYBER1 (1300 292 371).

Was this information helpful?

Popular pages

Essential Eight

Alerts and advisories

Information Security Manual

Australian Cyber Security Hotline

1300 CYBER1 (1300 292 371)

Contact us

View all content

Privacy

Disclaimer

Glossary

Copyright

Accessibility

Social media terms of use

Careers