Unitronics Cybersecurity Advisory 2023-001:

Default administrative password

Publication Date:	DEC 19th 2023
Update Date:	DEC 19th 2023
Version:	1.0
CVE	CVE-2023-6448

Summary

An unauthenticated attacker with network access can take administrative control of a vulnerable

Unitronics Vision and Samba series system, that uses a default administrative password.

Appearance

Component	Product	Affected product version
VisiLogic	Vision and Samba series	VisiLogic < 9.9.00 OS < 12.38

Description

An unauthenticated attacker with network access can take administrative control of a Unitronics Vision and Samba series systems programmed using VisiLogic version before 9.9.00 and use a default administrative password.

Mitigation

Disconnect the PLC from the open, unauthorized, internet access.

Update to the latest VisiLogic version, the patched version force:

- Changing the default administrative password.
- Setting a password on PCOM-enabled sockets.
- Controlling remote allowed PCOM operations using SDW10 roles.

If remote access is necessary, control network access to the PLC.

- Implement a Firewall/VPN in front of the PLC to control network access to the remote PLC.
- Use an allowlist of IPs for access.

More Unitronics recommended cybersecurity guidelines can be found on:
https://www.unitronicsplc.com/cyber_security_vision-samba/

Solution

Please update VisiLogic to the latest version (VisiLogic 9.9.00 and above, OS 12.38 and above) from the following link.

References

I. https://www.cisa.gov/news-events/ics-advisories/icsa-23-348-15
II. https://nvd.nist.gov/vuln/detail/CVE-2023-6448

Version History

Version	Date	Comments
1.0	DEC 19th 2023	Publication