Unitronics Cybersecurity Advisory 2024-009:
Vision™ Legacy, Storing Passwords in a Recoverable Format

Publication Date:	APRIL 25th 2024
Update Date:	MAY 1th 2024
Version:	1.0
CVE	CVE-2024-1480

Summary

Vision™ Legacy, Exploitable remotely/low attack complexity.
Thanks to the Dragos Cybersecurity Research team for the findings.

Appearance

Component	Product	Affected product version
Vision™ Legacy	Vision 230 Vision 280 Vision 290 Vision 530 Vision 120	All Versions

Description

Storing Passwords in a Recoverable Format.

Mitigation

Unitronics recommends users to:

1. Change the default 1111 "Info Mode" password via SI 253.
2. Restrict Ethernet access to the PLC having an Ethernet card using:
    a. Implementing PLC multi-factor access using SB 314.
    b. Apply a multi-factor VPN to protect the service from remote access.

Please follow Unitronics published recommendations or contact Unitronics technical support for more information.

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities, such as:

3. Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.
4. Locate control system networks and remote devices behind firewalls and isolate them from business networks.

When remote access is required, use more secure methods, such as virtual private networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

References

I. https://www.cisa.gov/news-events/ics-advisories/icsa-24-109-01
II. https://www.dragos.com/advisory/unitronics-vision-standard/

Version History

Version	Date	Comments
1.0	MAY 1th 2024	Publication