Unitronics Cybersecurity Advisory 2024-006:
OS Command Injection

Publication Date:	MARCH 18th 2024
Update Date:	MARCH 4th 2024
Version:	1.0
CVE	CVE-2024-27772

Summary

Remote code execution by an Unauthorized Actor.

Appearance

Component	Product	Affected product version
UniStream	All Products	UniLogic < 1.35.227

Description

An attacker can execute code from a remote location over an Ethernet network.

Mitigation

1. **Update to UniLogic version 1.35.227 or later.**
2. Verify that PLCs are not directly accessible from the Internet. Only allow access through specifically defined addresses or use VPN or ZTNA to access the devices.
3. Apply long complex passwords to devices. Change the default installed password.
4. Subscribe to UniCloud providing 2FA to allow access to devices, particularly for admin access.
5. Regularly check and update devices with the latest security updates.

Solution

Please update UniLogic to the latest version from the following link.

References

I. https://www.cisa.gov/sites/default/files/2023-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors-1.pdf

II. https://downloads.unitronicsplc.com/Sites/plc/Unilogic/UniLogic_1.35.227_January_2024.pdf

III. https://www.unitronicsplc.com/cyber_security_unistream/

IV. https://downloads.unitronicsplc.com/Sites/plc/support-tools-and-applications/Cyber-security-UniStream.pdf

Version History

Version	Date	Comments
1.0	MARCH 4th 2024	Publication