Unitronics Cybersecurity Advisory 2016-001: Stack-based buffer overflow

Publication Date:	MAY 5th 2016
Update Date:	JAN 2ND 2024
Version:	1.0
CVE	CVE-2016-4519

Summary

The failure is caused by an attempt to copy into a fixed-length stack buffer without validating its length.

Appearance

Component	Product	Affected product version
VisiLogic	Vision and Samba series	VisiLogic < 9.8.30

Description

Stack-based buffer overflow in Unitronics VisiLogic OPLC IDE before 9.8.30 allows remote attackers to execute arbitrary code via a crafted filename field in a ZIP archive in a VLP file.

Mitigation

Upgrade to Visilogic Version 9.8.30 or later to mitigate this vulnerability. The latest version can be found on the Unitronics website at the following location link.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs).

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

Solution

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

References

I. https://ics-cert.us-cert.gov/advisories/ICSA-16-175-02
II. http://zerodayinitiative.com/advisories/ZDI-16-375/

Version History

Version	Date	Comments
1.0	JAN 2th 2024	Publication