Unitronics Cybersecurity Advisory 2015-003: Heap-based buffer overflow in VisiLogic

Publication Date:	OCT 22th 2015
Update Date:	JAN 2ND 2024
Version:	1.0
CVE	CVE-2015-7939

Summary

Heap-based buffer overflow in Unitronics VisiLogic before 9.8.09 allows remote attackers to execute arbitrary code via a long VLP filename.

Appearance

Component	Product	Affected product version
VisiLogic	Vision and Samba series	VisiLogic < 9.8.09

Description

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Unitronics VisiLogic. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

A specific flaw exists within the parsing of VLP files. A specially crafted VLP will overrun a heap buffer and inject values past the end of the heap allocation. An attacker can leverage this vulnerability to execute arbitrary code under the context of a local Administrator.

Mitigation

Upgrade to Visilogic Version 9.8.09 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://www.zerodayinitiative.com/advisories/ZDI-16-001/
II. https://www.cisa.gov/news-events/ics-advisories/icsa-15-274-02a

Version History

Version	Date	Comments
1.0	JAN 2th 2024	Publication