Unitronics Cybersecurity Advisory 2015-001:
VisiLogic does not properly restrict access to ActiveX controls

Publication Date:	AUG 17th 2015
Update Date:	JAN 2ND 2024
Version:	1.0
CVE	CVE-2015-6478

Summary

Unitronics VisiLogic before 9.8.02 does not properly restrict access to ActiveX controls, which allows remote attackers to have an unspecified impact via a crafted website.

Appearance

Component	Product	Affected product version
VisiLogic	Vision and Samba series	VisiLogic < 9.8.02

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.

The specific flaw exists within the TeeCommander object in TeeChart5.ocx. A call to the ChartLink method of this object can cause arbitrary memory to be interpreted as an object. An attacker can leverage this vulnerability to execute arbitrary code under the context of the user.

Mitigation

Upgrade to Visilogic Version 9.8.02 or later to mitigate this vulnerability. The latest version can be found on the Unitronics website at the following location link.

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. http://www.zerodayinitiative.com/advisories/ZDI-15-573
II. http://www.zerodayinitiative.com/advisories/ZDI-15-577
III. http://www.zerodayinitiative.com/advisories/ZDI-15-578
IV. http://www.zerodayinitiative.com/advisories/ZDI-15-579
v. http://www.zerodayinitiative.com/advisories/ZDI-15-580

Version History

Version	Date	Comments
1.0	JAN 2th 2024	Publication