Unitronics Cybersecurity Advisory 2015-002: UniDownloader and VisiLogic ActiveX Control might cause remote execution code

Publication Date:	OCT 22th 2015
Update Date:	JAN 2ND 2024
Version:	1.0
CVE	CVE-2015-7905

Summary

Unitronics UniDownloader and Unitronics VisiLogic IPWorksSSL.HTTPS.1 ActiveX Control PostDataB/FirewallDataB Properties Remote Code Execution Vulnerability.

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 UniDownloader. 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 implementation of the WinSockPath property of the HTTPS ActiveX control. The control passes this property as the URL for a DLL to the LoadLibraryA API, which will automatically execute DllMain in the DLL. This can be leveraged by an attacker for remote code execution in the context of the process.

Mitigation

Upgrade to Visilogic Version 9.8.09 or later and the latest version of UniDownloader 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 and UniDownloader to the latest version from the following link.

References

I. http://www.zerodayinitiative.com/advisories/ZDI-15-574
II. http://www.zerodayinitiative.com/advisories/ZDI-15-575
III. http://www.zerodayinitiative.com/advisories/ZDI-15-576

Version History

Version	Date	Comments
1.0	JAN 2th 2024	Publication