Product Advisory

Product Family:	Productivity PLC	***Number:***	PA-PR-001
Part Numbers:	See affected part numbers table below	***Date Issued:***	05/22/2024
Subject:	Productivity PLC cyber security vulnerability	***Revision:***	Original

Purpose

This Product Advisory is related to Cyber Security and is intended to notify customers of a software or firmware vulnerability and to provide details on which products are impacted and explain how to mitigate the vulnerability or offer workarounds that can minimize the potential risk.

Affected Part Numbers

Additional Data			
Series	***CPU***	***Software***	***Firmware***
Productivity 3000	P3-550E	Software version 4.1.1.10 and prior	Firmware version 1.2.10.9 and prior
	P3-550		
	P3-530		
Productivity 2000	P2-550	Software version 4.1.1.10 and prior	Firmware version 1.2.10.10 and prior
Productivity 1000	P1-550	Software version 4.1.1.10 and prior	Firmware version 1.2.10.10 and prior
	P1-540		

Product Description

Productivity PLCs are programmable logic controllers designed for controlling industrial systems. They are programmed using Productivity Suite from AutomationDirect.com.

Vulnerability Classification

AutomationDirect rates the severity level of the known Vulnerabilities with a CVSS score of High.

Vulnerability Overview

AutomationDirect is aware of the following vulnerabilities in the products listed above:

Vulnerability #1 FiBurn heap-based buffer overflow vulnerability

A specially crafted network packet can lead to a buffer overflow. An attacker can send an unauthenticated packet to trigger this vulnerability.

Vulnerability #2 CurrDir heap-based buffer overflow vulnerability

A specially crafted network packet can lead to denial of service. An attacker can send an unauthenticated packet to trigger these vulnerability.

Vulnerability #3 FileSystem API out-of-bounds write vulnerabilities

Specially crafted network packets can lead to heap-based memory corruption. An attacker can send malicious packets to trigger these vulnerabilities.

Vulnerability #4 FileSelect stack-based buffer overflow vulnerability

A specially crafted network packet can lead to stack-based buffer overflow. An attacker can send an unauthenticated packet to trigger this vulnerability.

Product Advisory

Vulnerability Overview Cont'd

Vulnerability #5 Remote Memory Diagnostics Write-What-Where vulnerability

A specially crafted network packet can lead to an arbitrary write. An attacker can send an unauthenticated packet to trigger this vulnerability.

Vulnerability #6 Remote Memory Diagnostics Read-What-Where vulnerability

A specially crafted network packet can lead to a disclosure of sensitive information. An attacker can send an unauthenticated packet to trigger this vulnerability.

Vulnerability #7 Telnet Diagnostic Interface leftover debug code vulnerability

A specially crafted series of network requests can lead to unauthorized access. An attacker can send a sequence of requests to trigger this vulnerability.

Vulnerability #8 scan_lib.bin library code injection vulnerability

A specially crafted scan_lib.bin can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.

Remediations

Update the Productivity Suite programming software to version 4.2.0.x or higher.

Update Productivity PLC's firmware to the latest version.

Latest version of firmware/software can be found here:
https://www.automationdirect.com/support/software-downloads

Mitigations

Although Automation Networks and Systems come equipped with built-in password protection mechanisms, this represents a fraction of the security measures needed to safeguard these systems. It is imperative that Automation Control System Networks integrate data protection and security measures that match, if not exceed, the robustness of conventional business computer systems. We advise users of PLCs, HMI products, and SCADA systems to conduct a thorough network security analysis to ascertain the appropriate level of security necessary for their specific application.

AutomationDirect has identified the following mitigation for instances where systems cannot be upgraded to latest version:

- Physically disconnect the PLC from any external networks, including the internet, local area networks (LANs), and other interconnected systems.
- Configure network segmentation to isolate PLC from other devices and systems withing the organization.
- Implement firewall rules or network access control (NAC) policies to block incoming and outgoing traffic to the PLC.

Please refer to the following link for supporting information related to security considerations.
https://support.automationdirect.com/docs/securityconsiderations.pdf

Technical Assistance

If you have any questions regarding this Product Advisory, please contact Technical Support at 770-844-4200 or 800-633-0405 for further assistance.