

Security Bulletin XRX24-014

CVE-2024-47555

CVE-2024-47556/CVE-2024-47557

CVE-2024-47558/CVE-2024-47559

Xerox® FreeFlow® Core v7.0

Bulletin Date: October 1, 2024

Purpose

This Bulletin is intended ONLY for the specific software identified for security issues which have been rated at a level of IMPORTANT or higher.

Description

Xerox engineering and development has resolved multiple Remote Code Execution vulnerabilities found in FreeFlow Core version 7.0.

- CVE-2024-47555 (High) – User and System Configuration
- CVE-2024-47556 (High) and CVE-2024-47557 (High) – Pre-Auth RCE via Path Traversal
- CVE-2024-47558 (High) and CVE-2024-47559 (High) – Authenticated RCE via Path Traversal

Thank you to Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam) for working with Xerox Team to identify and mitigate these vulnerabilities.

Mitigation

Please consider upgrading to FreeFlow Core version 7.0.11 via the software available on Xerox.com [here](#).



© 2024 Xerox Corporation. All rights reserved. Xerox® and WorkCentre® are trademarks of Xerox Corporation in the United States and/or other countries.