Xerox Security Bulletin XRX25-002

Xerox® Workplace Suite®

Mitigations for CVE-2024-55925, CVE-2024-55926, CVE-2024-55927, CVE-2024-55928, CVE-2024-55929, CVE-2024-55930, CVE-2024-55931

Bulletin Date: January 23, 2025

Purpose

This Bulletin is intended ONLY for the specific software indicated for security issues rated with a criticality level of IMPORTANT or higher.

The following CVEs have been mitigated in Xerox® Workplace Suite ® version 5.6.701.9.

CVE ID	Vulnerability
CVE-2024-55925	API Security bypass through header manipulation
CVE-2024-55926	Arbitrary file upload through header manipulation
	Arbitrary file deletion on server through header manipulation
	Arbitrary file read on server through header manipulation
CVE-2024-55927	Flawed token generation implementation
	Hard-coded key implementation
CVE-2024-55928	Clear text secrets returned
	Remote system secrets in clear text
CVE-2024-55929	Mail spoofing
CVE-2024-55930	Weak default folder permissions
CVE-2024-55931	Token stored in session storage*

* Will be fixed in future release.

Acknowledgement

Thank you to Cyril Servières of Orange Cyberdefense for identifying these issues and Sébastien Desbordes of Airbus SE for his support.