THREAT BULLETINS

Security Researchers Discover and Disclose Two High-Severity Xerox FreeFlow Core Flaws

TLP:WHITE

Aug 14, 2025

On August 13, 2025, HORIZON3.ai security researchers published an Attack Blog regarding two high-severity vulnerabilities, CVE-2025-8355 and CVE-2025-8356, affecting Xerox FreeFlow Core version 8.0.4.

The security researchers discovered that these flaws could be exploited to execute Server-Side Request Forgery (SSRF) (CVE-2025-8355) and Remote Code Execution (RCE) (CVE-2025-8356) attacks. While there is no current evidence of active exploitation, these vulnerabilities pose a significant risk to infrastructure where vulnerable FreeFlow Core instances are implemented.

Health-ISAC provides this information to increase situational awareness, encourage users to assess their level of risk to these vulnerabilities, and apply the available patch to affected instances.

Analysis:

The vulnerabilities, CVE-2025-8355 and CVE-2025-8356, were disclosed on August 8, 2025, in Xerox Security Bulletin XRX25-013. The security flaws impact Xerox FreeFlow Core version 8.0.4, a key

software component for managing and automating document workflows.

Xerox printing and document management solutions are ubiquitous products that are likely used in hospitals, clinics, pharmacies, and health systems. These environments likely rely on these devices to produce everything from patient-facing materials and billing statements to internal administrative documents, potentially exposing them to these vulnerabilities.

Xerox has rated both vulnerabilities as of critical severity, with CVSS scores of 7.5 and 9.8, respectively, underscoring the critical risk they present.

The first vulnerability, CVE-2025-8355, is an XML External Entity (XXE) processing flaw that can be leveraged to conduct a Server-Side Request Forgery (SSRF) attack. By crafting a malicious XML payload, an attacker can force the vulnerable server to make unintended requests to internal resources. This can scan internal networks, access services that are not externally exposed, and exfiltrate sensitive information, bypassing perimeter security controls.

The second and more severe vulnerability, CVE-2025-8356, is a Path Traversal flaw that can lead to Remote Code Execution (RCE). This vulnerability allows an attacker to manipulate file path inputs to access directories and files outside the application's scope. Successful exploitation could allow an attacker to upload and execute arbitrary code on the server, resulting in the potential for a complete takeover of the affected system.

The criticality of these flaws and the potential for an attacker to conduct additional malicious activities following exploitation make this a significant and urgent threat.

Recommendations:

Organizations should immediately identify if they are using the affected Xerox FreeFlow Core software and, if so, patch it to version 8.0.5 as recommended by Xerox, in addition to the following:

- Continuously monitor for unusual activity and suspicious connections.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	horizon3, thehackernews, nist, nist 1, xerox, hhs

Alert ID bf127563

View Alert

Share Feedback

was this helpful? |

Tags FreeFlow Core, CVE-2025-8356, CVE-2025-8355, Xerox

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps.

Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**