Security Advisory 2023-025

Critical vulnerabilities in PaperCut

April 20, 2023 — v1.0

TLP:CLEAR

History:

- *20/04/2023 — v1.0 – Initial publication*

Summary

A new security advisory has been issued concerning two critical vulnerabilities in PaperCut MF/NG, which are actively being exploited in the wild. The vulnerabilities allow unauthenticated remote code execution and information disclosure. PaperCut users are strongly urged to update their software immediately to mitigate these risks. [1]

Technical Details

The first vulnerability, identified as `CVE-2023-27350` and `ZDI-CAN-18987 / PO-1216`, is an unauthenticated remote code execution flaw. This vulnerability affects both application and site servers. An attacker can exploit this flaw to execute arbitrary code on the affected server without any need for authentication, potentially leading to a complete compromise of the system. This vulnerability scores 9.8 on CVSS v3.1, classifying it as critical.

The second vulnerability, identified as `CVE-2023-27351` and `ZDI-CAN-19226 / PO-1219`, is an unauthenticated information disclosure flaw specifically for application servers. This vulnerability allows an attacker to access sensitive user information without authentication, potentially exposing data such as usernames, full names, email addresses, office/department information, and card numbers. Additionally, the attacker may retrieve hashed passwords for internally created PaperCut users. However, password hashes for users synced from directory sources like Microsoft 365, Google Workspace, and Active Directory remain unaffected. Although this vulnerability has not been observed being exploited, it is still essential to address it. The severity of this vulnerability is high, with a CVSS v3.1 score of 8.2.

Affected Products

CVE-2023–27350:

PaperCut MF or NG version 8.0 or later, on all OS platforms.

CVE-2023–27351:

PaperCut MF or NG version 15.0 or later, on all OS platforms.

Recommandations

Upgrade to PaperCut MF and PaperCut NG versions 20.1.7, 21.2.11, or 22.0.9 and later to address these vulnerabilities.

Detections

To check for exploitation, PaperCut recommends the following: [1]

- Look for suspicious activity in `Logs` > `Application Log`, within the PaperCut admin interface.
- Keep an eye out in particular for any updates from a user called `[setup wizard]`.
- Look for new (suspicious) users being created, or other configuration keys being tampered with.
- If the Application Server logs happen to be in debug mode, check to see if there are lines mentioning `SetupCompleted` at a time not correlating with the server installation or upgrade. Server logs can be found e.g., in `[app-path]/server/logs/*.*` where `server.log` is normally the most recent log file.

References

[1] https://www.papercut.com/kb/Main/PO-1216-and-PO-1219