PaperCut Warns of Exploited Vulnerability in Print Management Solutions

Print management solutions provider PaperCut has warned organizations that exploitation of a recently patched critical-severity vulnerability has commenced.

Papercut offers a print management system called PaperCut MF/NG, which provides monitoring and control capabilities. With PaperCut NG organizations can manage and control printing, while PaperCut MF allows them to manage and track off-the-glass copier activity.

Tracked as CVE-2023-27350 (CVSS score of 9.8), the exploited vulnerability is described as an improper access control issue in the SetupCompleted class of PaperCut MF/NG.

Successful exploitation of this security defect allows a remote, unauthenticated attacker to bypass authentication and execute arbitrary code with System privileges.

“We have confirmed that under certain circumstances this allows for an unauthenticated attacker to get remote code execution (RCE) on a PaperCut Application Server. This could be done remotely and without the need to log in,” PaperCut’s advisory reads.

The issue impacts PaperCut MF and NG versions 8.0 and later. The company patched the bug in March 2023 with the release of PaperCut MF and PaperCut NG versions 20.1.7, 21.2.11, and 22.0.9, and urges customers to update their installations as soon as possible, since exploitation has started.

“Please note that as of 18th April, 2023 we have evidence to suggest that unpatched servers are being exploited in the wild,” the company says. Both application servers and site servers are impacted.

PaperCut recommends reviewing server access logs and performing malware scans to identify any signs of suspicious activity resulting from the vulnerability’s exploitation.

“If you suspect that your server has been compromised, we recommend taking server backups, then wiping the Application Server, and rebuilding from a ‘safe’ backup point prior to when you discovered any suspicious behavior,” the company notes.

The vulnerability was reported to the vendor by an anonymous researcher through Trend Micro’s Zero Day Initiative (ZDI) in January. No information is available about the attacks exploiting CVE-2023-27350It’s currently unclear if the flaw was exploited with a zero-day status at some point.

Along with CVE-2023-27350, PaperCut also patched CVE-2023–27351, a high-severity flaw in PaperCut MF or NG versions 15.0 and later, which could allow an attacker to access user information such as usernames, names, emails, office information, and card numbers.

“The attacker can also retrieve the hashed passwords for internal PaperCut-created users only. This could be done remotely and without the need to log in,” PaperCut explains.

The bug exists within the SecurityRequestFilter class and is the result of an improperly implemented authentication algorithm. This vulnerability, also reported through ZDI, does not appear to be exploited in malicious attacks.

Related: Veritas Vulnerabilities Exploited in Ransomware Attacks Added to CISA ‘Must Patch’ List

Related:CISA Adds Chrome, macOS Bugs to Known Exploited Vulnerabilities Catalog

Related: Zimbra Flaw Exploited by Russia Against NATO Countries Added to CISA ‘Must Patch’ List

https://www.securityweek.com/papercut-warns-of-exploited-vulnerability-in-print-management-solutions/