Huntress: Most PaperCut Installations Not Patched Against Already-Exploited Security Flaw

Most Windows and macOS PaperCut installations have not been patched against a critical-severity vulnerability already exploited in attacks, according to a warning from endpoint and response security firm Huntress.

The security defect, tracked as CVE-2023-27350 (CVSS 9.8/10), is described as an improper access control bug in the PaperCut MF/NG print management system. Attackers can exploit the flaw to bypass authentication and execute arbitrary code remotely, with the privileges of the 'System' user.

In March 2023, PaperCut patched the vulnerability with the release of PaperCut MF and PaperCut NG versions 20.1.7, 21.2.11, and 22.0.9. Last week, the company warned that the issue was already exploited in malicious attacks, urging customers to update installations immediately.

Despite the urgency to update, however, most PaperCut MF/NG customers have yet to apply the available patches, Huntress said in a new report.

In the environments it protects, Huntress has identified more than 1,000 Windows hosts with PaperCut installed. Among them, there are over 900 vulnerable versions, spread across about 700 organizations.

The company also identified three macOS hosts with PaperCut

Server installed and says that two of them are running vulnerable versions. While PaperCut installations should not be accessible from the internet, a Shodan search shows that there are at least 1,800 publicly accessible PaperCut servers.

Exploitation of the critical PaperCut vulnerability, Huntress warns, started days before PaperCut's advisory and patch, with the attackers deploying copies of the legitimate Atera and Syncro remote management and maintenance (RMM) applications for persistent access to the vulnerable systems.

While analyzing a domain observed in these attacks, Huntress researchers identified a Windows DLL that proved to be a variant of the Truebot malware, a post-exploitation tool linked to Silence, a threat actor known to be associated with Russian hacking group TA505 – the threat actor behind the Cl0p ransomware.

While the ultimate goal of the current activity leveraging PaperCut's software is unknown, these links (albeit somewhat circumstantial) to a known ransomware entity are concerning. Potentially, the access gained through PaperCut exploitation could be used as a foothold leading to follow-on movement within the victim network, and ultimately ransomware deployment," Huntress notes.

The security firm also performed an analysis of vulnerable versions of PaperCut MF/NG and discovered that, once the print management solution has been installed, authentication can be bypassed by simply navigating to the 'SetupCompleted' page.

Without knowing any credentials, an attacker could exploit the bug to log in as an administrator, gaining access to all configurations and settings. The attacker could then make several tweaks to disable PaperCut MF/NG's sandbox and have Java code executed on the server.

The cybersecurity firm has created a working proof-of-concept (PoC) that demonstrates both how authentication can be

bypassed and how code can be executed remotely on vulnerable PaperCut servers.

Last week, the US Cybersecurity and Infrastructure Security Agency (CISA) added the PaperCut MF/NG vulnerability to its Known Exploited Vulnerabilities list.

Related: GoAnywhere MFT Zero-Day Exploitation Linked to Ransomware Attacks

Related: Russia-Linked TA505 Back at Targeting Financial Institutions

Related: FIN11 Spun Out From TA505 Umbrella as Distinct Attack Group

Huntress: Most PaperCut Installations Not Patched Against Already-Exploited Security Flaw