National Cyber Security Centre

2308080124-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Multiple Vulnerabilities in PaperCut NG/MF

Wednesday 9th August, 2023

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

PaperCut has released details of three vulnerabilities discovered in PaperCut NG/MF, which if exploited, could lead to privilege escalation and remote code execution.

Details were published by security researchers, alongside PaperCut, including information on recommended remediation and potential mitigation steps.

The advisory is available here:

https://www.papercut.com/kb/Main/SecurityBulletinJuly2023/

CVE-2023-3486:
A potential Denial of Service issue whereby an unauthenticated attacker with direct IP access to the system could upload files to a target directory. If exploited, this could fill up the system's disk space leading to reduced availability.

CVE-2023-39143:
Two path traversal vulnerabilities which, if exploited, could be leveraged to read and write arbitrary files. Remote Code Execution can be achieved with this vulnerability if the external device setting is enabled.

ZDI-CAN-21013:
A vulnerability affecting a third party dependency could be exploited to escalate privileges. Administrator access is required for this to be successfully exploited.

These vulnerabilities have been patched in PaperCut NG and PaperCut MF version 22.1.3.

Products Affected

- CVE-2023-3486: All PaperCut NG and MF versions prior to 22.1.3 on all OS platforms.
- CVE-2023-39143: All PaperCut NG and MF versions prior to 22.1.3 on Windows platforms only.
- ZDI-CAN-21013: All PaperCut NG and MF versions prior to 22.1.3 on all OS platforms.

  PaperCut has provided a list of components or products which are not affected. A comprehensive list can be found at the link below:

  https://www.papercut.com/kb/Main/SecurityBulletinJuly2023/

Impact

Exploitation of these vulnerabilities could allow an attacker to cause denial of service, escalate privileges, and gain unauthorised access to the target environment.

Recommendations

The NCSC strongly advises all affected organisations of the latest PaperCut NG/MF vulnerabilities to read the latest advisory from PaperCut, and apply the available patches.

Affected organisations should monitor the advisory for updates here:

https://www.papercut.com/kb/Main/SecurityBulletinJuly2023/

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie