PaperCut MF: Card truncation on HP readers

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-6180
State	PUBLISHED
Assigner	PaperCut
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-05 07:16:00 UTC
Updated	2026-05-05 07:16:00 UTC
Description	A race condition exists in PaperCut MF when processing badge-swipe data from certain HP multifunction devices. Under sp

Risk And Classification

Primary CVSS: v4.0 4.1 MEDIUM from eb41dac7-0af8-4f84-9f6d-0272772514f4

CVSS:4.0/AV:P/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-20 | CWE-367 | CWE-367 CWE-367 Time-of-check time-of-use (TOCTOU) race condition | CWE-20 CWE-20 Improper input validation

Version	Source	Type	Score	Severity	Vector
4.0	eb41dac7-0af8-4f84-9f6d-0272772514f4	Secondary	4.1	MEDIUM	CVSS:4.0/AV:P/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N
4.0	CNA	CVSS	4.1	MEDIUM	CVSS:4.0/AV:P/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N

CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

High

ntegrity

None

vailability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:P/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	PaperCut	PaperCut NG/MF	affected 24.1.9 semver	Not specified
CNA	PaperCut	PaperCut NG/MF	affected 25.0.10 semver	Not specified

References

Reference	Source	Link
www.papercut.com/kb/Main/papercut-ng-mf-and-papercut-hive-security-bulletin-ma...	eb41dac7-0af8-4f84-9f6d-0272772514f4	www.paper
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.