Pachno 1.0.6 Cross-Site Request Forgery via State-Changing Endpoints

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

Summary

CVE	CVE-2026-40041
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 19:16:51 UTC
Updated	2026-04-13 19:16:51 UTC
Description	Pachno 1.0.6 contains a cross-site request forgery vulnerability that allows attackers to perform arbitrary actions in authenti

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:L/SI:L/SA:L/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-352 | CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:L/SI:L/SA:
4.0	CNA	CVSS	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:L/SI:L/SA:
3.1	disclosure@vulncheck.com	Primary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

None

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:L/SI:L/SA:L/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pancho	Pachno	affected 1.0.6	Not specified

References

Reference	Source	Link	T
www.vulncheck.com/advisories/pachno-cross-site-request-forgery-via-state-changi...	disclosure@vulncheck.com	www.vulncheck.com	

www.zeroscience.mk/en/vulnerabilities/ZSL-2026-5983.php	disclosure@vulncheck.com	www.zeroscience.mk	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

Vendor Comments And Credit

Discovery Credit

CNA: LiquidWorm as Gjoko Krstic of Zero Science Lab (en)

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