ZEBRA: Consensus Divergence in Transparent Sighash Hash-Type Handling

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

Summary

CVE	CVE-2026-41583
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:41 UTC
Updated	2026-05-08 15:57:11 UTC
Description	ZEBRA is a Zcash node written entirely in Rust. Prior to zebrad version 4.3.1 and prior to zebra-script version 5.0.2, after a

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from security-advisories@github.com

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

EPSS: 0.000490000 probability, percentile 0.151940000 (date 2026-05-11)

Problem Types: CWE-573 | CWE-573 CWE-573: Improper Following of Specification by Caller

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N
4.0	CNA	DECLARED	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

None

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:H/SA:H/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	ZcashFoundation	Zebra	affected zebrad < 4.3.1	Not specified
CNA	ZcashFoundation	Zebra	affected zebra-script < 5.0.2	Not specified

References

Reference	Source	Link	Tags
github.com/ZcashFoundation/zebra/security/advisories/GHSA-8m29-fpq5-89jj	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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