



# Zebra has a Consensus Failure due to Improper Verification of V5 Transactions

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-34377
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 15:16:19 UTC
<b>Updated</b>	2026-04-01 14:24:02 UTC
<b>Description</b>	ZEBRA is a Zcash node written entirely in Rust. Prior to zebra version 4.3.0 and zebra-consensus version 5.0.1, a logic er

## Risk And Classification

**Primary CVSS:** v4.0 8.4 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000250000 probability, percentile 0.066040000 (date 2026-04-01)

**Problem Types:** CWE-347 | CWE-347 CWE-347: Improper Verification of Cryptographic Signature

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.4	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	8.4	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

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:H/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/MSX/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 < 4.3.0	Not specified
CNA	ZcashFoundation	Zebra-consensus	affected < 5.0.1	Not specified

References				
Reference	Source	Link	Tags	
github.com/ZcashFoundation/zebra/security/advisories/GHSA-3vmh-33xr-9cqh	security-advisories@github.com	github.com		
github.com/ZcashFoundation/zebra/releases/tag/v4.3.0	security-advisories@github.com	github.com		
zfn.org/zebra-4-3-0-critical-security-fixes-zip-235-support-and-perfo...	security-advisories@github.com	zfn.org		
CVE Program record	CVE.ORG	www.cve.org	canonical	
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,	

No vendor comments have been submitted for this CVE.

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

