Zero Motorcycles Firmware Key Exchange without Entity Authentication

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

Summary

CVE	CVE-2026-1354
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 22:16:18 UTC
Updated	2026-04-22 21:23:52 UTC
Description	Zero Motorcycles firmware versions 44 and prior enable an attacker to forcibly pair a device with the motorcycle via Bluetoc

Risk And Classification

Primary CVSS: v4.0 5.9 MEDIUM from ics-cert@hq.dhs.gov

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

EPSS: 0.000200000 probability, percentile 0.056230000 (date 2026-04-22)

Problem Types: CWE-322 | CWE-322 CWE-322

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	5.9	MEDIUM	CVSS:4.0/AV:A/AC:H/AT:P/PR:N/UI:P/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N/E:X
4.0	CNA	CVSS	5.9	MEDIUM	CVSS:4.0/AV:A/AC:H/AT:P/PR:N/UI:P/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N
3.1	ics-cert@hq.dhs.gov	Secondary	6.4	MEDIUM	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:H
3.1	CNA	CVSS	6.4	MEDIUM	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Zero Motorcycles	Zero Motorcycles Firmware	affected 44 custom	Not specified

References

Reference	Source	Link	Tags
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-11...	ics-cert@hq.dhs.gov	github.com	
www.cisa.gov/news-events/ics-advisories/icsa-26-111-06	ics-cert@hq.dhs.gov	www.cisa.gov	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Persephone Karnstein of Bureau Veritas Cybersecurity North America reported this vulnerability to CISA. (en)

Additional Advisory Data

Workarounds

CNA: Zero Motorcycles has investigated this report and cautions users to pair their mobile device to their vehicle in a safe location where they can be sure no one else will try to pair at the same time. Once initiated, complete the full pairing process and confirm it is successful. Store physical keys in a secure location and do not leave the bike unattended with the key in the "ON" position. Zero Motorcycles plans to address this issue in a firmware update scheduled for release in May 2026. Update the firmware to the latest available version.

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