America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Zero Motorcycles Firmware

Release Date: April 21, 2026 **Alert Code:** ICSA-26-111-06

RELATED TOPICS: INDUSTRIAL CONTROL SYSTEM VULNERABILITIES </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, INDUSTRIAL CONTROL SYSTEMS </topics/industrial-control-systems>

View CSAF <https://github.com/cisagov/csaf/blob/develop/csaf_files/ot/white/2026/icsa-26-111-06.json>

Summary

Successful exploitation of this vulnerability could allow an attacker to pair via Bluetooth with a motorcycle, gaining unauthorized access to all Bluetooth functions, including changing the firmware.

The following versions of Zero Motorcycles Firmware are affected:

- Zero Motorcycles firmware <=44 (CVE-2026-1354)

CVSS	Vendor	Equipment	Vulnerabilities
v3 6.4	Zero Motorcycles	Zero Motorcycles Firmware	Key Exchange without Entity Authentication

Background

- **Critical Infrastructure Sectors:** Transportation Systems
- **Countries/Areas Deployed:** Worldwide
- **Company Headquarters Location:** United States

Vulnerabilities

Expand All +

CVE-2026-1354 +

Acknowledgments

- Persephone Karnstein of Bureau Veritas Cybersecurity North America reported this vulnerability to CISA

Legal Notice and Terms of Use

This product is provided subject to this Notification (https://www.cisa.gov/notification) and this Privacy & Use policy (https://www.cisa.gov/privacy-policy).

Recommended Practices

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov/ics. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time. This vulnerability has a high attack complexity.

Revision History

- **Initial Release Date:** 2026-04-21

Date	Revision	Summary
2026-04-21	1	Initial Publication

Legal Notice and Terms of Use

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Tags

Sector: Transportation Systems Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector>

Topics: Industrial Control System Vulnerabilities </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, Industrial Control Systems </topics/industrial-control-systems>

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Related Advisories

APR 21, 2026 ■ ICS ADVISORY | ICSA-26-111-04

Siemens Analytics Toolkit </news-events/ics-advisories/icsa-26-111-04>

APR 21, 2026 ■ ICS ADVISORY | ICSA-26-111-02

Siemens RUGGEDCOM CROSSBOW Secure Access Manager Primary </news-events/ics-advisories/icsa-26-111-02>

APR 21, 2026 ■ ICS ADVISORY | ICSA-26-111-03

Siemens SINEC NMS </news-events/ics-advisories/icsa-26-111-03>

APR 21, 2026 ■ ICS ADVISORY | ICSA-26-111-12

SenseLive X3050 </news-events/ics-advisories/icsa-26-111-12>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov