America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

PX4 Autopilot

Release Date: March 31, 2026 **Alert Code:** ICSA-26-090-02

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-26-090-02.json>

Summary

Successful exploitation of this vulnerability could allow an attacker with access to the MAVLink interface to execute arbitrary shell commands without cryptographic authentication.

The following versions of PX4 Autopilot are affected:

- Autopilot v1.16.0_SITL_latest_stable (CVE-2026-1579)

CVSS	Vendor	Equipment	Vulnerabilities
v3 9.8	PX4	PX4 Autopilot	Missing Authentication for Critical Function

Background

- **Critical Infrastructure Sectors:** Transportation Systems, Emergency Services, Defense Industrial Base
- **Countries/Areas Deployed:** Worldwide
- **Company Headquarters Location:** Switzerland

Vulnerabilities

Expand All +

CVE-2026-1579 +

Acknowledgments

- Dolev Aviv of Cyviation 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.

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the Internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

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.

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

Do not click web links or open attachments in unsolicited email messages.

Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.

Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time.

Revision History

- **Initial Release Date:** 2026-03-31

Date	Revision	Summary
2026-03-31	1	Initial Publication

Legal Notice and Terms of Use

Tags

Sector: Defense Industrial Base Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/defense-industrial-base-sector>, Emergency Services Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/emergency-services-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

MAR 31, 2026 ■ ICS ADVISORY | ICSA-26-090-01

MAR 26, 2026 ■ ICS ADVISORY | ICSA-26-085-02

[Anritsu Remote Spectrum Monitor </news-events/ics-advisories/icsa-26-090-01>]

[OpenCode Systems OC Messaging and USSD Gateway </news-events/ics-advisories/icsa-26-085-02>]

MAR 26, 2026 ■ ICS ADVISORY | ICSA-26-085-03

[PTC Windchill Product Lifecycle Management </news-events/ics-advisories/icsa-26-085-03>]

MAR 26, 2026 ■ ICS ADVISORY | ICSA-26-085-01

[WAGO GmbH & Co. KG Industrial Managed Switches </news-events/ics-advisories/icsa-26-085-01>]

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

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>