PX4 Autopilot Missing authentication for critical function

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-1579
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 21:16:27 UTC
Updated	2026-04-01 14:23:37 UTC
Description	The MAVLink communication protocol does not require cryptographic authentication by default. When MAVLink 2.0 messag

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from ics-cert@hq.dhs.gov

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/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: 0.000730000 probability, percentile 0.222060000 (date 2026-04-02)

Problem Types: CWE-306 | CWE-306 CWE-306

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
3.1	ics-cert@hq.dhs.gov	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/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

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	PX4	Autopilot	affected v1.16.0 SITL	Not specified

References

Reference	Source	Link	Tags
docs.px4.io/main/en/mavlink/security_hardening	ics-cert@hq.dhs.gov	docs.px4.io	

docs.px4.io/main/en/mavlink/security_hardening	ics-cert@hq.dhs.gov	docs.px4.io	
www.cisa.gov/news-events/ics-advisories/icsa-26-090-02	ics-cert@hq.dhs.gov	www.cisa.gov	
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-09...	ics-cert@hq.dhs.gov	github.com	
docs.px4.io/main/en/mavlink/message_signing	ics-cert@hq.dhs.gov	docs.px4.io	
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: Dolev Aviv of Cyviation reported this vulnerability to CISA. (en)

Additional Advisory Data

Solutions

CNA: PX4 recommends enabling MAVLink 2.0 message signing as the authentication mechanism for all non-USB communication links. PX4 has published a security hardening guide for integrators and manufacturers at https://docs.px4.io/main/en/mavlink/security_hardening Message signing configuration documentation can be found at https://docs.px4.io/main/en/mavlink/message_signing

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