

Report

Cybersecurity Advisory for P-Net

Attachments

Contents

1 Overview	2
2 Affected Versions	2
3 Vulnerability Details	2
3.1 CVE-2026-111730	2
3.2 CVE-2026-111731	3
3.3 CVE-2026-111732	3
3.4 CVE-2026-111733	4
3.5 CVE-2026-111734	5
3.6 CVE-2026-111735	5
3.7 CVE-2026-111736	6
3.8 CVE-2026-112200	7
3.9 CVE-2026-115795	7
3.10 CVE-2026-115794	8
3.11 CVE-2026-115793	9
4 Mitigation Steps	9
5 Additional Information	9

1 Overview

This advisory covers several security vulnerabilities in P-Net versions prior to 1.0.3.

2 Affected Versions

- P-Net versions prior to 1.0.3

3 Vulnerability Details

3.1 CVE-2026-111730

CVE ID	CVE-2026-111730
Title	Out-of-bounds write in CheckPeers block parser due to unvalidated peer station name length
Description	P-Net before 1.0.3 does not validate the LengthPeerStationName field of a CheckPeers block in get_check_peer(). The received length (up to 255) was used to copy data into the 241-byte peer station name buffer and to place the terminating NUL byte, so a crafted block writes up to 15 bytes past the end of the buffer. This can lead to a crash (denial of service) or potentially arbitrary code execution. Requires establishment of session that needs ADJACENT network access.

CWE	CWE-787 (Out-of-bounds Write)
CVSS v4.0 Base Score	7.2 (High)
CVSS v4.0 Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N
Recommendation	Upgrade to P-Net 1.0.3 or later.
Reported by	Brian Willows, f0rw4rd (quellsec.dev)

Technical Details

The LengthPeerStationName field of a CheckPeers block was used unchecked as the copy size into the 241-byte peer station name buffer, and for the position of the terminating NUL. A length above 240 writes up to 15 bytes past the buffer.

Fix

The received name lengths are now validated against the sizes of the receiving buffers. The maximum size of PeerPortName was also corrected according to the specification.

3.2 CVE-2026-111731

CVE ID	CVE-2026-111731
Title	Infinite loop when reading PDPortDataCheck record of subslot 0
Description	P-Net before 1.0.3 enters an infinite loop when handling a read request for the PDPortDataCheck record with subslot 0 (whole module). The loop over the ports never advanced to the next port, so the request never completes and the device stops responding. A remote unauthenticated attacker can use this to cause a denial of service.
CWE	CWE-835 (Loop with Unreachable Exit Condition ('Infinite Loop'))
CVSS v4.0 Base Score	7.1 (High)
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/MAV:A/MA
Recommendation	Upgrade to P-Net 1.0.3 or later.
Reported by	f0rw4rd (quellsec.dev)

Technical Details

A read of the PDPortDataCheck record with subslot 0 used a special branch that looped over the ports without advancing to the next port, so the request never completed.

Fix

The special branch was removed, as it is not described in the PROFINET specification.

3.3 CVE-2026-111732

CVE ID	CVE-2026-111732
---------------	-----------------

Title	Out-of-bounds write when parsing AR Vendor Block requests
Description	P-Net before 1.0.3, when built with PNET_OPTION_AR_VENDOR_BLOCKS enabled, parses a data length from a field of the ARVendorBlock request that is not part of the block definition and uses it as the number of bytes to copy into a fixed-size buffer, without comparing it with the buffer size or the block length. A crafted Connect request causes an out-of-bounds write. This can lead to a crash (denial of service) or potentially arbitrary code execution. This option is disabled by default.
CWE	CWE-787 (Out-of-bounds Write)
CVSS v4.0 Base Score	7.5 (High)
CVSS v4.0 Vector	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/MAV:X/MA
Recommendation	Upgrade to P-Net 1.0.3 or later.
Reported by	f0rw4rd (quellsec.dev)

Technical Details

With PNET_OPTION_AR_VENDOR_BLOCKS enabled, the ARVendorBlock parser read a data length from a field that is not part of the block definition, and used it as the copy size into a fixed-size buffer.

Fix

The parser no longer extracts the non-existent field. The block length is used, and checked against the buffer size, before copying.

3.4 CVE-2026-111733

CVE ID	CVE-2026-111733
Title	NULL pointer dereference on implicit read of AR specific record index
Description	P-Net before 1.0.3 dereferences a NULL AR pointer when handling an implicit read request without a valid target AR UUID for a record index that requires an AR (AR specific indices 0xE000-0xEFFF, and the expected identification data of a slot or subslot). A remote unauthenticated attacker can send such a request to crash the device (denial of service).
CWE	CWE-476 (NULL Pointer Dereference)
CVSS v4.0 Base Score	7.1 (High)
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/MAV:A/MA
Recommendation	Upgrade to P-Net 1.0.3 or later.
Reported by	f0rw4rd (quellsec.dev)

Technical Details

An implicit read request without a target AR UUID was passed on for record indices that require an AR (0xE000-0xEFFF, and expected identification data), and the NULL AR pointer was dereferenced.

Fix

Such requests are now rejected with the corresponding PNIO status when no AR is given.

3.5 CVE-2026-111734

CVE ID	CVE-2026-111734
Title	Missing length validation of EtherType, VLAN and FrameID fields in pf_eth_rcv()
Description	P-Net before 1.0.3 does not validate the length of a received Ethernet frame in pf_eth_rcv() before reading the EtherType, any VLAN tags and the PROFINET FrameID. The VLAN tag loop had no upper bound, so a truncated frame, or a frame consisting only of VLAN tags, makes the function read past the end of the receive buffer. This can cause a crash (denial of service) or disclose memory content.
CWE	CWE-125 (Out-of-bounds Read)
CVSS v4.0 Base Score	7.1 (High)
CVSS v4.0 Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:H/SC:N/SI:N/SA:N
Recommendation	Upgrade to P-Net 1.0.3 or later.
Reported by	router0mail

Technical Details

pf_eth_rcv() read the EtherType, VLAN tags and FrameID without checking the frame length, and the VLAN tag loop had no upper bound.

Fix

The frame length is now checked before each field is read, and the VLAN tag loop is bounded by the frame length. Frames that are too short are dropped.

3.6 CVE-2026-111735

CVE ID	CVE-2026-111735
Title	Integer underflow leads to out-of-bounds read in pf_cpm_c_data_ind()

Description	P-Net before 1.0.3 contains an integer underflow in <code>pf_cpm_c_data_ind()</code> . When handling a received cyclic data frame while the consumer is in the FRUN or RUN state, the offset of the APDU status was computed as the frame length minus 4 using 16-bit arithmetic, without checking that the frame is long enough. A crafted short frame makes the offset wrap around, so the function reads outside the receive buffer. This can cause a crash (denial of service) or disclose memory content.
CWE	CWE-191 (Integer Underflow (Wrap or Wraparound)), CWE-125 (Out-of-bounds Read)
CVSS v4.0 Base Score	7.1 (High)
CVSS v4.0 Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:H/SC:N/SI:N/SA:N
Recommendation	Upgrade to P-Net 1.0.3 or later.

Technical Details

In `pf_cpm_c_data_ind()` the APDU status offset was calculated as frame length minus 4 in 16-bit arithmetic. For a frame shorter than 4 bytes the offset wraps around and points outside the receive buffer.

Fix

The frame length is now checked before the offset is calculated. Frames that are too short are dropped.

3.7 CVE-2026-111736

CVE ID	CVE-2026-111736
Title	NULL pointer dereference on implicit read of user specific record index
Description	P-Net before 1.0.3 dereferences a NULL AR pointer in <code>pf_fspm_cm_read_ind()</code> when handling an implicit read request without a valid target AR UUID for a user specific record index, if the application has registered a read callback. A remote unauthenticated attacker can send such a request to crash the device (denial of service).
CWE	CWE-476 (NULL Pointer Dereference)
CVSS v4.0 Base Score	7.1 (High)
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/MAV:A/MA
Recommendation	Upgrade to P-Net 1.0.3 or later.

Technical Details

For a user specific record index, an implicit read without a target AR UUID resulted in a NULL AR pointer being dereferenced in `pf_fspm_cm_read_ind()` before the application read callback was called.

Fix

A missing AR is now handled, as record data with a user specific index may or may not be related to an AR.

3.8 CVE-2026-112200

CVE ID	CVE-2026-112200
Title	Resource exhaustion from unreleased AR and RPC session on RPC requests with incorrect endianness
Description	P-Net before 1.0.3 does not release the Application Relationship (AR) and the RPC session when an RPC request is rejected because its data representation has incorrect endianness. The session and its AR remain allocated, so repeated requests exhaust the available sessions. Once they are exhausted the device no longer answers new RPC requests, including Connect, until it is restarted. A remote unauthenticated attacker can use this to cause a denial of service.
CWE	CWE-772 (Missing Release of Resource after Effective Lifetime)
CVSS v4.0 Base Score	7.1 (High)
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/MAV:A/MA
Recommendation	Upgrade to P-Net 1.0.3 or later.
Reported by	JianWeiHuang-stu

Technical Details

When an RPC request was rejected due to incorrect data representation (endianness), the AR and RPC session allocated for it were not released.

Fix

The AR and the session are now released when the request is rejected.

3.9 CVE-2026-115795

CVE ID	CVE-2026-115795
Title	Out-of-bounds read of DCP block header in DCP Set and Identify request parsing
Description	P-Net before 1.0.3 does not check that a complete block header is present in the received data before reading the next block in DCP Set and Identify requests. If the last block ends at the end of the receive buffer, the block length of the following block is read past the end of the buffer. In addition, a DCP Set block with a length smaller than the two-byte block qualifier makes the length underflow, so the block is processed with a length of 65534 bytes. This can cause a crash (denial of service) or disclose a small amount of memory content. Requires ADJACENT network access.

CWE	CWE-125 (Out-of-bounds Read)
CVSS v4.0 Base Score	5.3 (Medium)
CVSS v4.0 Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N
Recommendation	Upgrade to P-Net 1.0.3 or later.
Reported by	Aditya Gupta - adi0x90

Technical Details

The DCP Set and Identify parsing loops read the header of the next block without checking that it fits in the received data. A DCP Set block shorter than the two-byte block qualifier made the block length underflow to 65534.

Fix

The DCP header and block headers are now read with bounds checked parser functions, and requests that are too short are dropped. DCP Set blocks too short to contain the qualifier are rejected.

3.10 CVE-2026-115794

CVE ID	CVE-2026-115794
Title	Alarm data length not validated against received frame length
Description	P-Net before 1.0.3 passes the application alarm callback a data length derived from the variable part length field of a received RTA alarm frame without checking it against the length of the received frame. A short frame can make the callback receive a length of up to 65507 bytes. An application that copies the reported number of bytes reads past the end of the receive buffer. The attacker must have established an Application Relationship and requires ADJACENT network access. Applications that do not use the alarm data are not affected.
CWE	CWE-130 (Improper Handling of Length Parameter Inconsistency)
CVSS v4.0 Base Score	2.3 (Low)
CVSS v4.0 Vector	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N
Recommendation	Upgrade to P-Net 1.0.3 or later.
Reported by	Aditya Gupta - adi0x90

Technical Details

The data length given to the application alarm callback was derived from the variable part length of a received RTA alarm frame, without checking it against the received frame length.

Fix

The alarm data is now copied to a stack buffer using a bounds checked function that fails if the data is not within the received frame or does not fit. The alarm is dropped on failure and the callback gets the validated copy.

3.11 CVE-2026-115793

CVE ID	CVE-2026-115793
Title	Resource exhaustion from RPC sessions kept for requests to unknown interface
Description	P-Net before 1.0.3 does not release the RPC session allocated for an RPC request that names an unknown interface or object UUID, and does not start a timeout for it. Repeated requests with different activity UUIDs exhaust the available sessions. Once they are exhausted the device no longer answers new RPC requests, including Endpoint Mapper Lookup and Connect, until it is restarted. A remote unauthenticated attacker can use this to cause a denial of service.
CWE	CWE-772 (Missing Release of Resource after Effective Lifetime)
CVSS v4.0 Base Score	7.1 (High)
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/MAV:A
Recommendation	Upgrade to P-Net 1.0.3 or later.
Reported by	Aditya Gupta - adi0x90

Technical Details

An RPC request naming an unknown interface or object UUID allocated a new session that was never released, and no timeout was started for it. Each request with a new activity UUID consumed one session.

Fix

The session is now killed after the response has been sent.

4 Mitigation Steps

Upgrade to P-Net 1.0.3 or later. All vulnerabilities are fixed in that release. As an alternative measure and to enhance security, ensure that devices are not connected to public networks. Devices that are not accessible to attackers, such as those on isolated networks or protected by firewalls, are at significantly reduced risk.

5 Additional Information

For further inquiries or support, please contact:

- **Support Contact:** support@rt-labs.com
- **Website:** <https://www.rt-labs.com>

Disclaimer: This advisory is provided for informational purposes only. RT-Labs is not liable for any damage caused by the exploitation of the vulnerabilities listed.