Report

Cybersecurity Advisory for P-Net

Attachments

RT-LABS

RT-Labs AB
Andra Långgatan 46
SE-413 27 Göteborg
Sweden

info@rt-labs.com
www.rtlabs.com

Contents

1 Overview **2**

2 Affected Versions **2**

3 Vulnerability Details **2**
3.1 CVE-2026-124758 . . . 2
3.2 CVE-2026-124759 . . . 3
3.3 CVE-2026-124760 . . . 4
3.4 CVE-2026-124761 . . . 5
3.5 CVE-2026-124762 . . . 5
3.6 CVE-2026-127122 . . . 6
3.7 CVE-2026-127123 . . . 7
3.8 CVE-2026-127124 . . . 8
3.9 CVE-2026-127125 . . . 9

4 Mitigation Steps **9**

5 Additional Information **9**

1 Overview

This advisory covers several security vulnerabilities in P-Net versions prior to 1.0.4. Two of them, CVE-2026-124759 and CVE-2026-124762, are only partly fixed in 1.0.4 and have a remaining risk, which is described for each of them.

2 Affected Versions

- P-Net versions prior to 1.0.4
- P-Net versions 1.0.4 and later

3 Vulnerability Details

3.1 CVE-2026-124758

CVE ID	CVE-2026-124758
Title	Integer underflow of the record data length in IODWrite requests

Description	P-Net before 1.0.4 does not check the record data length of an IODWrite request to a non-user record index against the size of the record block header. The 32-bit length is reduced by the header size before it is passed to the record handlers, so a length smaller than the header underflows and the handlers receive a data length of about 65530. The fixed-size reads of the I&M and PDPort handlers can then read past the end of the session buffer. The result of the write is discarded. The attacker must have an established Application Relationship or be able to send in the context of one, and requires ADJACENT network access.
CWE	CWE-191 (Integer Underflow (Wrap or Wraparound))
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:N/VI:N/VA:L/SC:N/SI:N/SA:N
Recommendation	Upgrade to P-Net 1.0.4 or later.
Reported by	3ntr0py1337, Khalilov M

Technical Details

The record data length of an IODWrite request is a 32-bit value from the frame. The block header size was subtracted from it before it was checked, so a value below 6 underflowed and was truncated to a data length of about 65530 for the record handlers.

Fix

The record data length is compared with the bytes that remain in the arguments of the request, without arithmetic that can wrap around. A record data length that does not fit is rejected as “ArgsLength invalid”, and a record of a non-user index that is too short to contain the block header is rejected as a write length error.

3.2 CVE-2026-124759

CVE ID	CVE-2026-124759
Title	Alarm frames are accepted from any source address
Description	P-Net before 1.0.4 routes a received RTA alarm frame to an Application Relationship using only the destination alarm reference in the frame, without checking the source of the frame. A host with ADJACENT network access can abort an established Application Relationship with a single alarm ERROR frame, or deliver forged alarm notifications with chosen type, slot, subslot, USI and payload to the application.
CWE	CWE-346 (Origin Validation Error)
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:N/VI:L/VA:H/SC:N/SI:N/SA:N

Recommendation	Upgrade to P-Net 1.0.4 or later, which ignores alarm frames that do not come from the IO-controller of the Application Relationship. It reduces the risk but does not remove it, see Remaining Risk.
Reported by	Aditya Gupta (Attify - attify.com)

Technical Details

An RTA alarm frame was routed to an Application Relationship by the destination alarm reference in the frame. The source address and the source alarm reference were not checked.

Fix

The source address of the frame is compared with the address of the IO-controller of the Application Relationship, and the source reference with the alarm reference of the IO-controller. Frames from other sources are ignored.

Remaining Risk

The frames are not authenticated and the specification defines the alarm channel only by the addressing of the frame. The address of the IO-controller is visible on the network and the alarm references are 16-bit values that are sent in clear in the connect. A host with ADJACENT network access that knows them can still send an alarm ERROR frame that aborts the Application Relationship, or forged alarm notifications. Isolate the network of the device.

3.3 CVE-2026-124760

CVE ID	CVE-2026-124760
Title	Alarm receiver stops delivering alarms after a malformed alarm notification
Description	P-Net before 1.0.4 sets the alarm receiver state to waiting for confirmation before the data of a received alarm notification is parsed. If the parsing fails the state is not restored, and later alarm notifications of the same priority are discarded without acknowledge until the Application Relationship is released. The Application Relationship and the cyclic data exchange keep working. The attacker must be able to send an alarm notification in the context of an established Application Relationship and requires ADJACENT network access.
CWE	CWE-754 (Improper Check for Unusual or Exceptional Conditions)
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:N/VI:N/VA:L/SC:N/SI:N/SA:N
Recommendation	Upgrade to P-Net 1.0.4 or later.
Reported by	Aditya Gupta (Attify - attify.com)

Technical Details

The alarm receiver was set to waiting for confirmation before the alarm data was parsed. A parse failure never cleared the state, and there is no timer.

Fix

The alarm notification is parsed before it is acknowledged and the state is changed. A frame that cannot be parsed is dropped.

3.4 CVE-2026-124761

CVE ID	CVE-2026-124761
Title	A DCP Set of the IP suite that is refused is still stored
Description	P-Net before 1.0.4 copies the IP suite of a DCP Set request to the current and the non-volatile configuration, and starts saving it, before the state of the device is checked. If the request is refused, for example because an Application Relationship is active, the configuration is not restored and is still saved. After a restart the device uses the refused address, and may not answer the controller or may use its address. A host with ADJACENT network access can use this while an Application Relationship is active.
CWE	CWE-696 (Incorrect Behavior Order)
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:N/VI:L/VA:H/SC:N/SI:N/SA:N
Recommendation	Upgrade to P-Net 1.0.4 or later.
Reported by	Aditya Gupta (Attify - attify.com)

Technical Details

The IP suite of a DCP Set request was stored in the current and the non-volatile configuration, and the save was queued, before the CMINA state was checked. A refused request did not restore them.

Fix

The configuration is changed, and saved, only when the DCP Set request is accepted.

3.5 CVE-2026-124762

CVE ID	CVE-2026-124762
Title	RPC reject, fault and cancel PDUs abort an Application Relationship

Description	P-Net before 1.0.4 finds the RPC session of a received PDU by its activity UUID only, and a reject, fault or cancel PDU for the session aborts the Application Relationship, without checking that the PDU is the answer to a call of the device or where it comes from. A host with ADJACENT network access that has observed the activity UUID of the connection, which is sent in clear in every RPC request, can abort the Application Relationship with one PDU. It also allocates a session for an unknown activity UUID and changes the address stored for an existing session.
CWE	CWE-346 (Origin Validation Error)
CVSS v4.0 Base Score	6.0 (Medium)
CVSS v4.0 Vector	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
Recommendation	Upgrade to P-Net 1.0.4 or later, which only handles a reject or fault as the answer to a call of the device and ignores a cancel. It reduces the risk but does not remove it, see Remaining Risk.
Reported by	Aditya Gupta (Attify - attify.com)

Technical Details

The RPC session of a received PDU was found by the activity UUID only. A reject, fault or cancel PDU aborted the Application Relationship of the session, an unknown activity UUID allocated a session, and the source address of the session was overwritten by every request.

Fix

A reject or fault is only handled if it is the answer to the call that the device has sent last, identified by the activity UUID and the sequence number, and is otherwise ignored without allocating or changing a session. A cancel no longer aborts the Application Relationship.

Remaining Risk

The source address of the sender is not checked, as DCE RPC identifies a client by its activity UUID and a call by the activity UUID and sequence number, and the PROFINET specification does not bind a call to an address. A host that has observed the activity UUID and the sequence number of the pending call of the device, which are in the RPC header, can still answer it with a reject or fault and abort the Application Relationship, as long as the session of the call exists. Isolate the network of the device.

3.6 CVE-2026-127122

CVE ID	CVE-2026-127122
Title	Out-of-bounds write with too many MCR blocks in a Connect request

Description	P-Net before 1.0.4 does not check the number of MCR request blocks in a Connect request against the number of multicast communication relations that an Application Relationship has room for (PNET_MAX_MC_CR, 1 by default). Each further block is written past the end of the array, into the rest of the Application Relationship and, with more blocks, into the following one. The written data comes from the request. No established Application Relationship is needed, and the attacker requires ADJACENT network access. Builds with PNET_OPTION_MC_CR disabled are not affected.
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 1.0.4 or later.

Technical Details

The MCR request blocks of a Connect request were stored in an array of the Application Relationship with room for PNET_MAX_MC_CR blocks. The index was the number of blocks received so far, and it was not checked against the size of the array.

Fix

A Connect request with more MCR request blocks than PNET_MAX_MC_CR is rejected with “Wrong block count”, before the block is stored.

3.7 CVE-2026-127123

CVE ID	CVE-2026-127123
Title	Fragment with another data representation releases an Application Relationship
Description	P-Net before 1.0.4 releases the Application Relationship of an RPC session, without the abort procedure, when a fragment of a request has another data representation (endianness) than the first fragment of the call. The application is not told that the Application Relationship is gone, the cyclic data stops, and the resources of the Application Relationship are left referencing a cleared structure. Another host can then connect in its place. A host with ADJACENT network access that has observed the activity UUID of the connection, which is sent in clear in every RPC request, can do this with one PDU.
CWE	CWE-404 (Improper Resource Shutdown or Release)

CVSS v4.0 Base Score	6.0 (Medium)
CVSS v4.0 Vector	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:H/SC:N/SI:N/SA:N
Recommendation	Upgrade to P-Net 1.0.4 or later.

Technical Details

When a fragment of a request had another data representation than the first fragment of the call, the Application Relationship of the session was freed directly, without the abort procedure that informs the application and closes the cyclic data, the alarms and the timers.

Fix

The call is rejected with nca_proto_error and the fragment is not added. The Application Relationship is not affected.

3.8 CVE-2026-127124

CVE ID	CVE-2026-127124
Title	RPC session pool exhausted by unfinished fragmented requests
Description	P-Net before 1.0.4 keeps the RPC session that is allocated for a fragment of a request with an unknown activity UUID, without a timeout, when the rest of the request never arrives. A session that does not get an Application Relationship is also kept after the response. Repeated fragments or requests with different activity UUIDs exhaust the available sessions, one UDP packet per session. Once they are exhausted the device no longer answers a Connect request until it is restarted. An unauthenticated attacker with ADJACENT network access 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:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
Recommendation	Upgrade to P-Net 1.0.4 or later.

Technical Details

A fragment of a request allocated a session that was only released when the request was complete. A session that did not get an Application Relationship was not released after the response, a ping or a PDU of an unexpected type.

Fix

On a session without an Application Relationship, the rest of a fragmented request is awaited for 8 s, after which the session is released. Such a session is also released after the response, a ping or a PDU of an unexpected type, unless an Endpoint Mapper lookup sequence or the resends of a fragmented response are in progress.

3.9 CVE-2026-127125

CVE ID	CVE-2026-127125
Title	NULL pointer dereference when a response fragment is not acknowledged
Description	P-Net before 1.0.4 aborts the Application Relationship of an RPC session when a fragment of a response has been resent without being acknowledged, without checking that the session has an Application Relationship. A request for an existing Application Relationship that is sent on another activity than its Connect, and gets a fragmented response, is handled on a session without one. If the response is not acknowledged, a NULL pointer is dereferenced and the device crashes. A conformant IO-controller does not send such requests. The attacker must have observed the AR UUID of an established Application Relationship and requires ADJACENT network access.
CWE	CWE-476 (NULL Pointer Dereference)
CVSS v4.0 Base Score	6.0 (Medium)
CVSS v4.0 Vector	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
Recommendation	Upgrade to P-Net 1.0.4 or later.

Technical Details

When the resends of a response fragment had been sent without an acknowledgement, the Application Relationship of the session was aborted without a check that the session has one.

Fix

A session without an Application Relationship is released instead. This is a defensive check, as a conformant IO-controller does not send a request for an Application Relationship on a session without it.

4 Mitigation Steps

Upgrade to P-Net 1.0.4 or later. CVE-2026-124758, CVE-2026-124760, CVE-2026-124761, CVE-2026-127122, CVE-2026-127123, CVE-2026-127124 and CVE-2026-127125 are fixed in that release. CVE-2026-124759 and CVE-2026-124762 are only partly fixed, see the remaining risk of each. 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.