Report

Cybersecurity Advisory for P-Net

Attachments

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

Contents

1 Overview **2**

2 Affected Versions **2**

3 Vulnerability Details **2**

3.1 CVE-2025-32396 . . . 2
3.2 CVE-2025-32397 . . . 3
3.3 CVE-2025-32398 . . . 3
3.4 CVE-2025-32399 . . . 3
3.5 CVE-2025-32400 . . . 4
3.6 CVE-2025-32401 . . . 4
3.7 CVE-2025-32402 . . . 4
3.8 CVE-2025-32403 . . . 5
3.9 CVE-2025-32404 . . . 5
3.10 CVE-2025-32405 . . . 5

4 Mitigation Steps **6**

5 Acknowledgements **6**

6 Additional Information **6**

1 Overview

This advisory addresses cybersecurity vulnerabilities discovered in the P-Net Profinet stack. The vulnerabilities may allow denial of service, and require immediate action to mitigate potential exploitation.

P-Net devices located on networks that are isolated from potential attackers, such as internal networks or those protected by firewalls, are not vulnerable to the identified threats.

2 Affected Versions

- P-Net versions 0.1.0, 1.0.0, and 1.0.1

3 Vulnerability Details

3.1 CVE-2025-32396

CVE ID	CVE-2025-32396
Description	Heap-based buffer overflow
Impact	Denial of service

Exploitability	This vulnerability can be exploited by a remote attacker capable of sending a malicious Connect RPC packet to an IO Device using the P-Net library
CVSS v3.1 Base Score	7.5
CVSS v3.1 Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Recommendation	Upgrade to P-Net version 1.0.2

3.2 CVE-2025-32397

CVE ID	CVE-2025-32397
Description	Heap-based buffer overflow
Impact	Denial of service
Exploitability	The vulnerability can be exploited by a remote attacker capable of sending a malicious Connect RPC packet to an IO Device using the P-Net library
CVSS v3.1 Base Score	7.5
CVSS v3.1 Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Recommendation	Upgrade to P-Net version 1.0.2

3.3 CVE-2025-32398

CVE ID	CVE-2025-32398
Description	NULL pointer derefence
Impact	Denial of service
Exploitability	The vulnerability can be exploited by a remote attacker capable of sending a malicious Read RPC packet to an IO Device using the P-Net library.
CVSS v3.1 Base Score	7.5
CVSS v3.1 Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Recommendation	Upgrade to P-Net version 1.0.2

3.4 CVE-2025-32399

CVE ID	CVE-2025-32399
Description	Unchecked input for loop condition
Impact	Denial of service

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

Exploitability	The vulnerability can be exploited by a remote attacker capable of sending RPC packets to an IO Device using the P-Net library
CVSS v3.1 Base Score	5.3
CVSS v3.1 Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
Recommendation	Upgrade to P-Net version 1.0.2

3.5 CVE-2025-32400

CVE ID	CVE-2025-32400
Description	Heap-based buffer overflow
Impact	Denial of service
Exploitability	The vulnerability can be exploited by a remote attacker capable of sending RPC packets to an IO Device using the P-Net library
CVSS v3.1 Base Score	7.5
CVSS v3.1 Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Recommendation	Upgrade to P-Net version 1.0.2

3.6 CVE-2025-32401

CVE ID	CVE-2025-32401
Description	Heap-based buffer overflow
Impact	Denial of service
Exploitability	The vulnerability can be exploited by a remote attacker capable of sending malicious RPC packets to an IO Device using the P-Net library
CVSS v3.1 Base Score	7.5
CVSS v3.1 Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Recommendation	Upgrade to P-Net version 1.0.2

3.7 CVE-2025-32402

CVE ID	CVE-2025-32402
Description	Out-of-bounds write
Impact	Denial of service, Data integrity

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

Exploitability	The vulnerability can be exploited by a remote attacker capable of sending malicious RPC packets to an IO Device using the P-Net library
CVSS v3.1 Base Score	7.5
CVSS v3.1 Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Recommendation	Upgrade to P-Net version 1.0.2

3.8 CVE-2025-32403

CVE ID	CVE-2025-32403
Description	Out-of-bounds write
Impact	Denial of service, Data integrity
Exploitability	The vulnerability can be exploited by a remote attacker capable of sending malicious RPC packets to an IO Device using the P-Net library
CVSS v3.1 Base Score	4.8
CVSS v3.1 Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L
Recommendation	Upgrade to P-Net version 1.0.2

3.9 CVE-2025-32404

CVE ID	CVE-2025-32404
Description	Out-of-bounds write
Impact	Denial of service, Data integrity
Exploitability	The vulnerability can be exploited by a remote attacker capable of sending malicious RPC packets to an IO Device using the P-Net library
CVSS v3.1 Base Score	4.8
CVSS v3.1 Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L
Recommendation	Upgrade to P-Net version 1.0.2

3.10 CVE-2025-32405

CVE ID	CVE-2025-32405
Description	Out-of-bounds write
Impact	Denial of service, Data integrity

Exploitability	The vulnerability can be exploited by a remote attacker capable of sending malicious RPC packets to an IO Device using the P-Net library
CVSS v3.1 Base Score	7.5
CVSS v3.1 Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Recommendation	Upgrade to P-Net version 1.0.2

4 Mitigation Steps

Affected users are advised to upgrade to P-Net version 1.0.2 to mitigate identified vulnerabilities.

As an alternative measure and to enhance security, ensure that P-Net 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 safeguarded against potential threats.

5 Acknowledgements

We acknowledge the efforts of Luca Borzacchiello from Nozomi Networks who identified and reported these vulnerabilities.

6 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.