VDE-2026-027: Phoenix Contact: Multiple vulnerabilities in the firmware of IOL MA8 EIP DI8 and IOL MA8 PN DI8 devices

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Wed Sep 16 08:00:00 CEST 2026	Engine: 2.6.11
Current release date: Wed Sep 16 08:00:00 CEST 2026	Build Date: Wed Sep 09 14:10:54 CEST 2026
Current version: 1.0.0	Status: FINAL
CVSSv3.1 Base Score: 9.8	Severity: Critical
Original language:	Language: en-GB
Also referred to: VDE-2026-027, PCSA-2026-00003	

Summary

The firmware of IOL MA8 EIP DI8 and IOL MA8 PN DI8 devices is affected by security vulnerabilities that can be used to bypass authentication. Code can be executed on the devices through command injection and local file inclusion. Path traversal and modified schemata can be used to read sensitive information such as password hashes or private keys from the devices.

General Recommendation

For general information and recommendations on security measures to protect network-enabled devices, refer to the application note: Application Note Security.

Impact

Authentication can be bypassed. Code with high access rights can be executed on the device so that the integrity of the device can be falsified. Sensitive information can be read out.

Mitigation

- Minimize network exposure for affected products and ensure that they are not accessible via the Internet.
- Isolate affected products from the corporate network.
- If remote access is required, use secure methods such as virtual private networks (VPNs).

Remediation

Phoenix Contact strongly recommends to update affected devices to firmware version 1.7.8.

Affected Product(s)

Article	Name	Affected	Fixed
1072838	IOL MA8 PN DI8	firmware <1.7.4	Firmware 1.7.8
1072839	IOL MA8 EIP DI8	firmware <1.7.4	Firmware 1.7.8

Acknowledgments

Phoenix Contact GmbH & Co. KG thanks the following parties for their efforts:

- CERT@VDE for coordination (see: https://certvde.com)
- Gabriele Quagliarella, Luca Borzacchiello from Nozomi Networks for reporting (see: https://nozominetworks.com/)

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- PCSA-2026-00003 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- Phoenix Contact application note (EXTERNAL): https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf
- VDE-2026-027: Phoenix Contact: Multiple vulnerabilities in the firmware of IOL MA8 EIP DI8 and IOL MA8 PN DI8 devices - HTML (SELF): https://certvde.com/en/advisories/VDE-2026-027
- VDE-2026-027: Phoenix Contact: Multiple vulnerabilities in the firmware of IOL MA8 EIP DI8 and IOL MA8 PN DI8 devices - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2026/vde-2026-027.json

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	Wed Sep 16 08:00:00 CEST 2026	Initial release.

Sharing rules

TLP:WHITE
For the TLP version see https://www.first.org/tlp/

Vulnerability Details

Remote code execution via uploading a malicious IODD file (CVE-2026-27565)

CVE Description

An unauthenticated remote attacker can upload a malicious IODD file that places and executes a shell script with root privileges. The shell script remains active even after a reboot.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Command Injection via PUT in /api/datastorage/data (CVE-2026-27564)

CVE Description

A high-privileged remote attacker can exploit a command injection vulnerability in the /api/datastorage/data endpoint by sending a PUT request with admin credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Gabriele Quagliarella from Nozomi Networks for reporting

Command Injection via GET in /api/datastorage/data (CVE-2026-27563)

CVE Description

A high-privileged remote attacker can exploit a command injection vulnerability in the /api/datastorage/data endpoint by sending a crafted GET request with admin credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Gabriele Quagliarella from Nozomi Networks for reporting

Command Injection via PUT in /api/iodd/config (CVE-2026-27562)

CVE Description

A high-privileged remote attacker can exploit a command injection vulnerability in the /api/iodd/config endpoint by sending a crafted PUT request with admin credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Gabriele Quagliarella from Nozomi Networks for reporting

Command Injection via GET in /api/iodd/config (CVE-2026-27561)

CVE Description

A high-privileged remote attacker can exploit a command injection vulnerability in the /api/iodd/config endpoint by sending a crafted GET request with admin credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Gabriele Quagliarella from Nozomi Networks for reporting

Command Injection via DELETE in /api/status/data (CVE-2026-27560)

CVE Description

A high-privileged remote attacker can exploit a command injection vulnerability in the /api/status/data endpoint by sending a crafted DELETE request with admin credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Command Injection via GET in /api/status/data (CVE-2026-27559)

CVE Description

A low-privileged remote attacker can exploit a command injection vulnerability in the /api/status/data endpoint by sending a crafted GET request with user credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Command Injection in /index.php/attached_devices_tab/ajax_remove_uploaded_iodd_files (CVE-2026-27558)

CVE Description

A low-privileged remote attacker can exploit a command injection vulnerability in the /index.php/attached_devices_tab/ajax_remove_uploaded_iodd_files endpoint using operator credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Path Traversal in /index.php/view_uploaded_iodd_file (CVE-2026-27557)

CVE Description

An unauthenticated remote attacker can exploit a path traversal vulnerability in the /index.php/view_uploaded_iodd_file endpoint allowing the SSH server's private keys to be read.

CWE:	CWE-35: Path Traversal: '.../...//'

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Local File Inclusion in /index.php/ajax/save_iodd_parameters (CVE-2026-27556)

CVE Description

A low-privileged remote attacker can exploit a local file inclusion vulnerability in the /index.php/ajax/save_iodd_parameters endpoint using a valid operator cookie allowing execution of arbitrary PHP code on the device.

CWE:	CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Local File Inclusion in /index.php/ajax/get_iodd_port_info (CVE-2026-27555)

CVE Description

A low-privileged remote attacker can exploit a local file inclusion vulnerability in the /index.php/ajax/get_iodd_port_info endpoint using a valid user cookie allowing execution of arbitrary PHP code on the device.

CWE:	CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Command Injection in /index.php/ajax/save_iodd_parameters (CVE-2026-27554)

CVE Description

A low-privileged remote attacker can exploit a command injection vulnerability in the /index.php/ajax/save_iodd_parameters endpoint using operator credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Information Disclosure via Schema Path Manipulation (CVE-2026-27553)

CVE Description

A low-privileged remote attacker can manipulate the schema path parameter in the /index.php/diagnostics_tab/ajax_diag_table_rows endpoint using a valid user cookie allowing disclosure of all user password hashes.

CWE:	CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	6.5
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	6.5

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Unauthorized IODD File Upload due to Improper Authorization (CVE-2026-27552)

CVE Description

A low-privileged remote attacker can exploit improper authorization in the /index.php/attached_devices_tab/do_upload endpoint to upload IODD files to the device, potentially altering device behavior or causing system crashes.

CWE:	CWE-863: Incorrect Authorization

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H	8.1
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H	8.1

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Command Injection in /index.php/ajax/parameterManage (CVE-2026-27551)

CVE Description

A low-privileged remote attacker can exploit a command injection vulnerability in the /index.php/ajax/parameterManage endpoint using user credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Command Injection in Field_Shadow_Password Class (CVE-2026-27550)

CVE Description

A low-privileged remote attacker can exploit a command injection vulnerability in the Field_Shadow_Password class using operator credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Command Injection in /index.php/attached_devices_tab/do_upload (CVE-2026-27549)

CVE Description

A low-privileged remote attacker can exploit a command injection vulnerability in the /index.php/attached_devices_tab/do_upload endpoint using operator credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Command Injection in /index.php/ajax/get_iodd_port_info (CVE-2026-27548)

CVE Description

A low-privileged remote attacker can exploit a command injection vulnerability in the /index.php/ajax/get_iodd_port_info endpoint using user or operator credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Command Injection in /index.php/ajax/get_iodd_menu_info (CVE-2026-27547)

CVE Description

A low-privileged remote attacker can exploit a command injection vulnerability in the /index.php/ajax/get_iodd_menu_info endpoint using valid user or operator credentials allowing execution of commands with root privileges on the device.

CWE:	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting

Authentication Bypass in _account_log (CVE-2026-27546)

CVE Description

An unauthenticated remote attacker can exploit an authentication bypass in the _account_log function to log in as an admin, even when accounts are properly configured.

CWE:	CWE-288: Authentication Bypass Using an Alternate Path or Channel

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
firmware <1.7.4 installed on IOL MA8 PN DI8 Order number: 1072838	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
firmware <1.7.4 installed on IOL MA8 EIP DI8 Order number: 1072839	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8

Fixed

Product
Firmware 1.7.8 installed on IOL MA8 PN DI8 Order number: 1072838 (Download)
Firmware 1.7.8 installed on IOL MA8 EIP DI8 Order number: 1072839 (Download)

Acknowledgments

- Luca Borzacchiello from Nozomi Networks for reporting