Product Security Advisory

June 18, 2026

InHand-PSA-2026-06

CVE-2026-38714, CVE-2026-38715,
CVE-2026-38716,CVE-2026-38717,
CVE-2026-38718

Overview

InHand Networks has confirmed the vulnerabilities impacting IR912, and IR915 Industrial Routers, and is providing measures to address these security vulnerabilities. Certain security vulnerabilities exist in these products that remote attackers could exploit to execute arbitrary commands (gaining root privileges) or cause denial of service attacks on the affected devices.

InHand Networks recommends that customers update the firmware version of the corresponding device models to the version that fixes the currently known security vulnerabilities.

Affected Products and Versions

InHand Networks has identified and addressed several security vulnerabilities in the following Industrial Router models and firmware versions:

Model	Affected Firmware Versions	Fixed Firmware Versions
IR912	IR9-V1.0.0.r20042 and prior	IR9-V1.0.0.r20044
IR915	IR9-V1.0.0.r20042 and prior	IR9-V1.0.0.r20044

Impact

These vulnerabilities, if exploited, could allow remote attackers to gain root privileges or cause denial of service on the affected devices.

- CVE-2026-38714: Command Injection in Python Configuration Function

  A command injection vulnerability exists in the Python configuration function of the affected products. This vulnerability could allow an attacker to obtain root privileges on the remote target device.
- CVE-2026-38715: Command Injection in Log Viewing Function

  A command injection vulnerability exists in the log viewing function of the affected products. This vulnerability could allow an attacker to obtain root privileges on the remote target device.
- CVE-2026-38716: Command Injection in Python Application Export Function

  A command injection vulnerability exists in the Python application export function of the affected products. This vulnerability could allow an attacker to obtain root privileges on the remote target device.
- CVE-2026-38717: Command Injection in File Upload Function

  A command injection vulnerability exists in the file upload function of the affected products. This vulnerability could allow an attacker to obtain root privileges on the remote target device.

- CVE-2026-38718: Buffer Overflow in Device Registration Function

  A buffer overflow vulnerability exists in the device registration function of the affected products. This vulnerability could allow an attacker to cause a denial of service attack on the remote target device.

Mitigation

InHand Networks strongly recommends customers update their affected devices to the corresponding fixed firmware versions:

- IR912: Download and upgrade to IR9-V1.0.0.r20044.
- IR915: Download and upgrade to IR9-V1.0.0.r20044.

Acknowledgements

Jincheng Wang, Professor Le Yu from Nanjing University of Posts and Telecommunications and Professor Xiapu Luo from Hong Kong Polytechnic University

Initial Publication Date

June 18, 2026

Resources

Security Solutions Website - https://www.inhand.com/en/compliance/product-security-advisories/