Product Security Advisory

May 28, 2026

InHand-PSA-2026-05

CVE-2026-38702, CVE-2026-38703,
CVE-2026-38704,CVE-2026-38705,
CVE-2026-38707

Overview

InHand Networks has confirmed the vulnerabilities impacting IR302, IR305, IR315, and IR615 Industrial Routers, and is providing measures to address these security vulnerabilities. Certain security vulnerabilities exist in these products that remote attackers could exploit to disable security features, execute arbitrary commands, or arbitrarily delete files 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
IR302	InRouter3XX-V3.5.108 and prior	InRouter3XX-V3.5.112
IR305	InRouter3X5-V1.0.118 and prior	InRouter3X5-V1.0.121
IR315	InRouter3X5-V1.0.118 and prior	InRouter3X5-V1.0.121
IR615	InRouter6XS-V1.0.118 and prior	InRouter6XS-V1.0.121

Impact

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

- CVE-2026-38702: Command Injection in Management Control Functions
  A command injection vulnerability exists in the management control functions of the affected products. This vulnerability could allow an attacker to obtain root privileges on the remote target device.
- CVE-2026-38703: Command Injection in ZeroTier VPN Function
  A command injection vulnerability exists in the ZeroTier VPN function of the affected products. This vulnerability could allow an attacker to obtain root privileges on the remote target device.
- CVE-2026-38704: Command Injection in WireGuard VPN Function
  A command injection vulnerability exists in the WireGuard VPN function of the affected products. This vulnerability could allow an attacker to obtain root privileges on the remote target device.
- CVE-2026-38705: Command Injection and Buffer Overflow in Digital I/O Function
  Command injection and buffer overflow vulnerabilities exist in the digital I/O function of the affected products. These vulnerabilities could allow an attacker to

obtain root privileges on the remote target device or cause a denial of service attack.

- CVE-2026-38707: Command Injection in IPSec VPN Function
  A command injection vulnerability exists in the IPSec VPN function of the affected products. This vulnerability could allow an attacker to obtain root privileges on the remote target device.

Mitigation

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

- IR302: Download and upgrade to InRouter3XX-V3.5.112.
- IR305: Download and upgrade to InRouter3X5-V1.0.121.
- IR315: Download and upgrade to InRouter3X5-V1.0.121.
- IR615: Download and upgrade to InRouter6XS-V1.0.121.

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

May 28, 2026

Resources

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