# Release Notes for Cisco IC3000 Industrial Compute Gateway for Release 1.4.2

**First Published:** 2023-03-12

**Last Modified:** 2023-03-14

## Introduction

The following release notes support the Cisco IC3000. These release notes are updated to describe new features, limitations, troubleshooting, recommended configurations, caveats, and provide information on how to obtain support and documentation.

## Image Information and Supported Platforms

**Note** You must have a Cisco.com account to download the software.

The Cisco IC3000 operates on the following Cisco IOS images:

- IC3000-K9-1.4.2.SPA

## Software Downloads

The latest image file for the IC3000 can be found here:

https://software.cisco.com/download/home/286321941/type/286322235/release/1.4.2

## Major Enhancements

Release 1.4.2 has no major enhancements.

## Related Documentation

The following documentation is available:

- Cisco IC3000 Industrial Compute Gateway
- Cisco IoT Field Network Director
- Cisco IOx
- Cisco IOx Developer information

# Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

**Note** You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account .

FND release notes are found here:

https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/products-release-notes-list.html

IOx release notes are found here:

https://www.cisco.com/c/en/us/support/cloud-systems-management/iox/products-release-notes-list.html

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ .

## Open Caveats

There are no open caveats for release 1.4.2.

## Resolved Caveats

The following table lists resolved caveats for release 1.4.2:

| Item | Description |
|---|---|
| CSCwd07668 | **Headline**: Backport CAF PSIRT's to 15M<br>**Symptoms**: A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system.<br>**Workaround**: Customers who do not want to use the Cisco IOx application hosting environment can disable IOx permanently on the device using the no iox configuration command. |

# Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

## Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

## Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.