

Field Notice: FN74158 – Limited Number of Cisco 1100 Integrated Services Routers

- [Products Affected](#)
- [Problem Description](#)
- [Problem Symptom](#)
- [Workaround/Solution](#)

Updated: April 4, 2025 Document ID: FN74158

[Bias-Free Language](#)



Impact Rating: Critical
First Published: 2024-Oct-02
Last Published: 2025-Apr-04
Revision: 2.0
Cisco Bug IDs: CSCwk59794

Notice

THIS FIELD NOTICE IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE FIELD NOTICE OR MATERIALS LINKED FROM THE FIELD NOTICE IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS FIELD NOTICE AT ANY TIME.

Products Affected

Affected Product Name	Description	Comments
C1109-4PLTE2P	ISR 1109 M2M 4P GE Ethernet, LTE Adv and DUAL Pluggables	
ISR1100-6G	ISR1100 Router, 4 GE LAN/WAN Ports and 2 SFP ports, 4GB RAM	
ISR1100-6GPM20	Promo – ISR1100 Router, 4GE LAN/WAN and 2 SFP ports, 4GB RAM	

Defect Information

Defect ID	Headline
CSCwk59794	Limited Number of Cisco Routers May Experience Memory Module Failures

Problem Description

A limited number of dynamic random-access memory (DRAM) components in Cisco 1100 Integrated Services Routers that are shipped from Cisco are impacted by a known issue in the memory supplier's manufacturing process. This issue can result in a higher rate of failure.

Background

In this case, a manufacturing deviation in specific DRAM components was contained to a specific date range. Since the discovery of this deviation, additional limits have been imposed on the manufacturing process to help prevent future components from experiencing this process variation.

Problem Symptom

Most memory components in the affected Cisco ISR1100 Routers with this manufacturing deviation will exhibit persistent, correctable memory errors. If left untreated, the affected units can eventually encounter an uncorrectable memory event. If encountered during runtime, uncorrectable errors may cause an unexpected reset.

The issue can result in a failure to boot to Cisco IOS Software after a crash, reload, or upgrade, resulting in the following error message on the front panel console port that is repeated every 5 minutes:

```
Initializing Hardware...
Initializing Hardware...
Initializing Hardware...
```

▼ Workaround/Solution

Cisco recommends replacement of the affected Cisco ISR1100 Routers in order to avoid potential device failure. For information about requesting a replacement, see the **Upgrade Program Information** section of this field notice after validating the serial number(s) of the affected units as described in the **How to Identify Affected Products** section of this field notice.

Important notes for replacement orders:

- The replacement orders are proactive replacements and do not adhere to normal service-level agreements or service contracts. Furthermore, some countries have strict importation regulations. For these reasons, extended lead time may occur for these replacements.
- The replacement devices will not ship with any accessories or modular parts such as cables, rack mounts, power supplies, network modules, or fans, just like any regular Return Material Authorization (RMA). All non-faulty components will need to be swapped from the old device to the replacement device.
- Customers can raise a return-only RMA when they are ready to return the faulty devices by following the instructions in the **Additional Information** section of this field notice.

▼ How to Identify Affected Products

To determine if a serial number is affected, see the Serial Number Validation section of this field notice.

▼ Additional Information

Use the following link to raise a return-only RMA: Support Case Manager (cisco.com)

To initiate a return RMA, use the following steps:

1. Select **Return of Defective Asset**.
2. Select **Return Queries** for the Request Type.
3. Select **New Services Return – RMA Needed** for the Sub-Request Type.
4. In the **Additional Request Details** field, enter the following information and submit the return-only RMA request:
TAC SR number: (not mandatory)
Customer CCO ID:
Contract Number: (not mandatory)
Part ID(s):
Serial Number:
Company Name:
Country:
Street Address:
State/Province:
Zip/Postal Code:
City:
On-site Contact Name:
On-site Contact Phone number:
On-site Contact E-mail:
Reason for RMA Creation: **FN# FN74158**
Bill to ID: (not mandatory)

Serial Number Validation

Cisco provides the Serial Number Validation Tool to verify whether a device is impacted by this issue. To check the device, enter the

serial number in the Serial Number Validation Tool.

Important: For security reasons, you must click the **Serial Number Validation Tool** link that is provided in this section. Do not copy and paste the link into a browser. Use of the Serial Number Validation Tool URL external to this field notice will fail.

Upgrade Program Information

Support Case Manager (SCM) must be used for ordering replacement parts for this Field Notice. To open SCM in a new tab, click the following link:

<https://mycase.cloudapps.cisco.com/fieldnotice?fn=FN74158>

SCM will validate eligibility and ensure that a request for a particular serial number has not already been submitted. If there is already a request, SCM will indicate that an **RMA has already been submitted and NOT eligible for replacement**.

Provide the following information:

- Affected serial numbers. Note that a serial number entitlement check may be performed.
- One ship-to address per request.
- Service Request number (SR#). This is not required, but if one exists, enter it for better tracking purposes.

Order entry supports up to 50 serial numbers per request. For more than 50, submit additional requests.

For questions about order status, see the Field Notice Affected Hardware Replacement FAQ.

Revision History

Version	Description	Section	Date
2.0	Added C1109-4PLTE2P to the list of affected product identifiers (PIDs).	Products Affected	2025-APR-04
1.0	Initial Release	—	2024-OCT-02

For More Information

For further assistance or for more information about this field notice, contact the Cisco Technical Assistance Center (TAC) using one of the following methods:

- Open a service request on Cisco.com
- By email or telephone

Receive Email Notification About New Field Notices

To receive email updates about Field Notices (reliability and safety issues), Security Advisories (network security issues), and end-of-life announcements for specific Cisco products, set up a profile in My Notifications.

Quick Links

About Cisco

Contact Us

Careers

Connect with a partner

Resources and Legal

[Feedback](#)

[Help](#)

[Terms & Conditions](#)

[Privacy](#)

[Cookies / Do not sell or share my personal data](#)

[Accessibility](#)

[Trademarks](#)

[Supply Chain Transparency](#)

[Newsroom](#)

[Sitemap](#)



©2025 Cisco Systems, Inc.