Critical Infrastructure Information Notice- CIIN-08-291-01

October 17, 2008

Possible Counterfeit Cisco Routers

US-CERT is aware of recent open source reports regarding possible counterfeit Cisco routers. US-CERT originally reported this activity in April 2006. Please note that US-CERT is re-releasing that information in this report for situational awareness purposes due to the new open source reporting and to provide methods for determining if a router is counterfeit.

Overview

Certain routers in the Cisco 2600 Router Series (2610XM, 611XM, 2620XM, 2621XM) and Cisco 1721 Modular Routers may be counterfeit. Cisco Systems has provided US-CERT with detailed information to assist organizations in determining if a router is counterfeit. Organizations may wish to check their 2600 and 1721 series routers. If organizations discover suspect counterfeit routers, they should contact US-CERT accordingly.

Detailed Instructions from CISCO Systems

The following sections provide screening procedures for detecting anomalies that indicate that a Cisco unit is counterfeit. Final determination as to the status of a router may only be made in coordination with Cisco Systems.

Product Anomaly Inspection: Cisco 2600 Router Series: (2610XM, 2611XM, 2620XM, 2621XM)

This section provides screening procedures for the Cisco 2600 Series Routers. If the following anomalies are found, the unit is counterfeit.

Defect 1: Microprocessor Model Number

Description: The design for the Cisco 2600 routers specifies a microprocessor component at position **U22** of the PCB. The standard-compliant processors all have part numbers with the letter "D" as the second-to-last character, such as **XPC860PZP50*D*4**. Certain counterfeit units have microprocessors with a "B" as the second-to-last character, such as **XPC860TZP50*B*5.** The "B" indicates a lesser feature set.

Figure 1 depicts a counterfeit part number while Figure 2 shows a Cisco compliant part number.

Figure 1. 2600XM: Certain counterfeit units use an incorrect microprocessor at U22, with a part number that has a "B" as the second-to-last character.

Figure 2. 2600XM: Compliant units use a microprocessor at U22 of the PCB whose part number has a "D" as the second-to-last character, such as XPC860PZP50D4.

Action: Check for the correct part number, with a "D" as the second-to-last character, on the surface of the microprocessor at position U22 of the PCB. A unit with a character other than a "D" as the second-to-last character is counterfeit.

(Tracking Code: 2600XM-U22PN)

Defect 2: PCB Part Number Incorrect

Description: The PCB on genuine Cisco 2600XM units bears a part number sticker reading **73-7YYY-XX,** (where *yyy* represents the exact model (see table below), and *xx* is a number representing the version). Certain counterfeit units either bear a part number sticker with an incorrect 73-level assembly part number, or no 73-level part number sticker.

Refer to the following table to match the labeled product model with the PCB Assembly part number.

Table I. Product Models with PCB Assembly Part Number

Labeled Product Model	PCB Assembly Part Number
2610XM	73-**7677**-XX
2611XM	73-**7679**-XX
2620XM	73-**7753**-XX
2621XM	73-**7754**-XX

Action: Use the table to verify that the PCB assembly part number sticker indicates the correct part number for the product model. For example, a genuine Cisco 2620XM will have a part number sticker on the PCB that reads *3-7753-XX*. The product model is indicated by markings on the front side of the unit, and on the compliance label affixed to the bottom of the chassis.

Consider a 2600-series router counterfeit if the PCB has a 73-level PCB assembly part number other than that indicated in the above table as correct for the model.

(Tracking Code: 2600XM-PCBPN)

Product Anomaly Inspection: Cisco 1721 Modular Router

This section provides screening procedures for the Cisco 1721 10/100 Modular Router. If any of the following anomalies are found, the unit may be counterfeit.

The following table shows the attributes to examine in a Cisco 1721 10/100 modular route in order to detect counterfeit units.

Table II. Cisco 1721 Modular Router Product Inspection: Summary of Attributes

Product ID	Location	Observation	Standards Problem	Visual / Functional	Tools Required	Approx. Time	Tracking Code
1721 Router	Chassis Shell (Internal)	RFI Screens	Unit without metal RFI screens in top and bottom shell is a flag.	Visual	Eyes	15 seconds.	**1721-RFIScreens**
	PCB	Incorrect Processor	Unit with "B" version of processor is a flag.	Visual	Eyes	15 seconds	**1721-U13Proc**
	PCB	Incorrect PLD	Altera PLD part not EPM7128AETC100-7 is a flag.	Visual	Eyes	15 seconds	**1721-Altera**
	Chassis Sides	Vent Casting	Horizontal cast ribs that do not extend to rear of chassis are a flag.	Visual	Eyes	15 seconds	**1721-SideCase**
	Chassis Top (Internal)	Unapproved Fan	Unit without part number on chassis fan is a flag.	Visual	Eyes	15 seconds	**1721-Fan**
	PCB	Incorrect Silkscreen	Test point label misspelled "JTAC" is a flag.	Visual	Eyes	15 seconds	**1721-TestPoints**

Figure 3 shows a global view of location attributes.

7-Altera
PLD Chip

6-JTAC
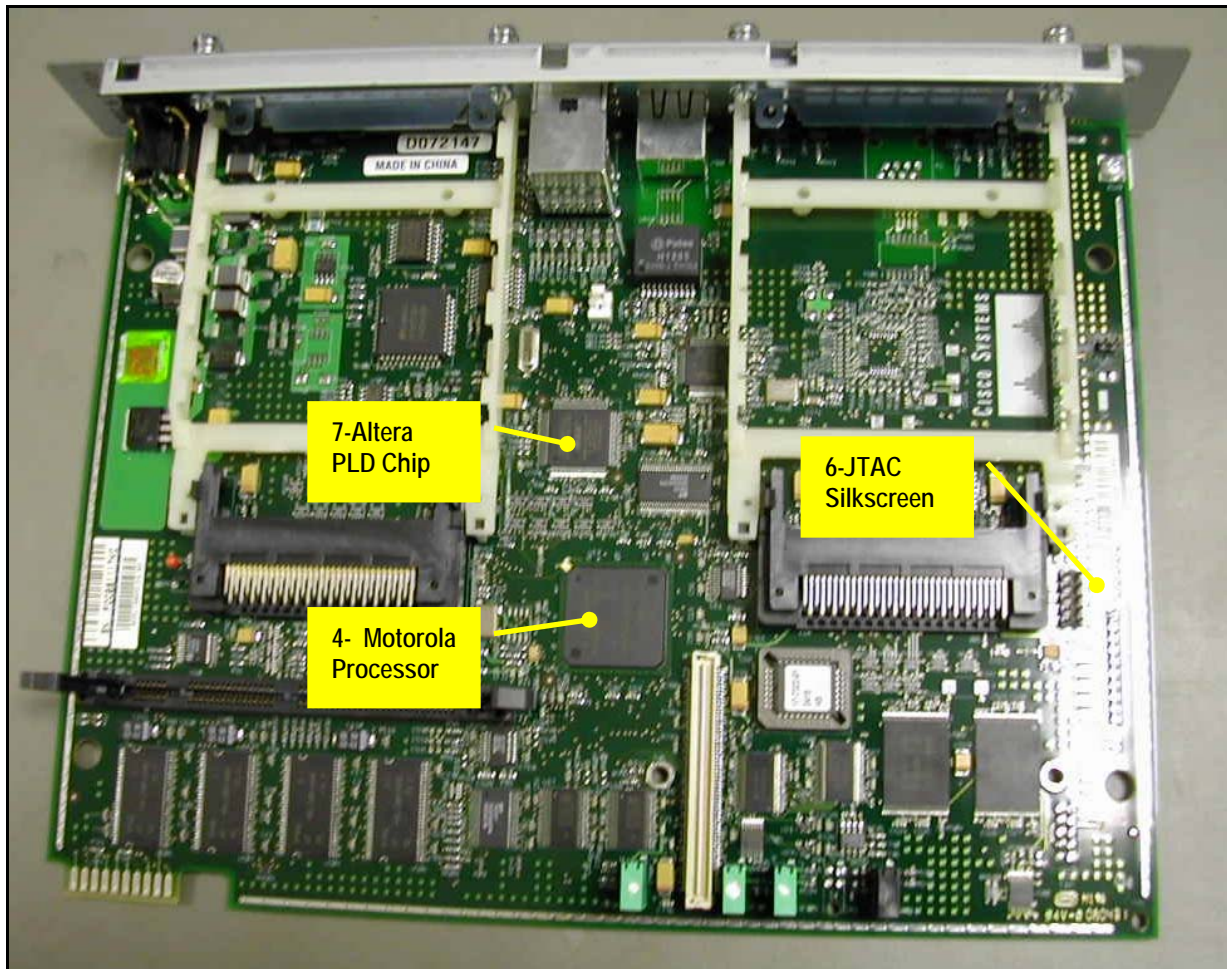Silkscreen

4- Motorola
Processor

Figure 3. Cisco 1721 Router (Internal PCB)

Defect 1: No RFI Screens in Top and Bottom of Chassis

Description: The Cisco 1721 Router has metal Radio Frequency Interference (RFI) mitigation screens in the top and bottom halves of the chassis shell. The following illustrations depict compliant and non-complaint Cisco 1720 chassis shells.
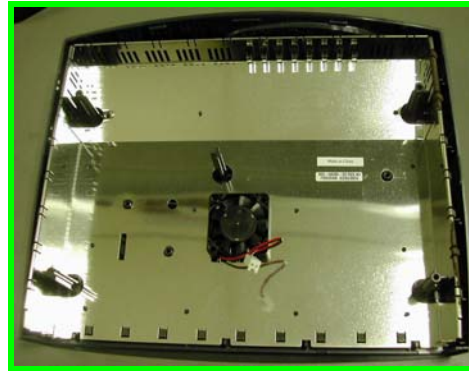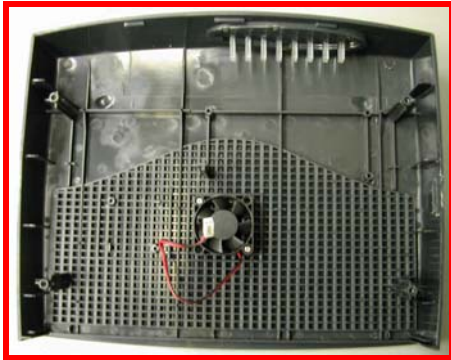
Non-compliant 1721 chassis   **Compliant 1721 chassis**

Figure 4. Compliant Cisco 1721 router has metal RFI shielding.

Action: Divert Cisco 1721 product that has no metal RFI screens in the top and bottom of the chassis.

Defect 2: Motorola Chip Not Version 'D'

Description: The design for the Cisco 1721 specifies a particular Motorola processor at position **U13** of the PCB, with part number **XPC860PZP50D4.** Certain non-compliant units have a similar processor with part number, with the letter **B** in the next to last position. Only a version **D** chip is correct. A unit that uses version 'B' of the chip is non-compliant.

Figure 5. 1721: Non-compliant version 'B' Motorola processor.

Figure 6. 1721: Compliant Motorola processor, with "D" revision.

Action: Examine the Motorola processor at position **U13** of the PCB. Divert Cisco 1721 product with a "B" version of this as potential counterfeit.

Defect 3: Altera PLD Chip Wrong Version

Description: The design for the Cisco 1721 Router specifies an Altera PLD with part number **EPM7128AETC100-7** in position **U714** on the top of the motherboard. Certain non-compliant units have an Altera part of an incorrect version and speed grade. The part number on these chips is often either **EPM7128AETC100-5** or **EPM7128AETC100-10**.
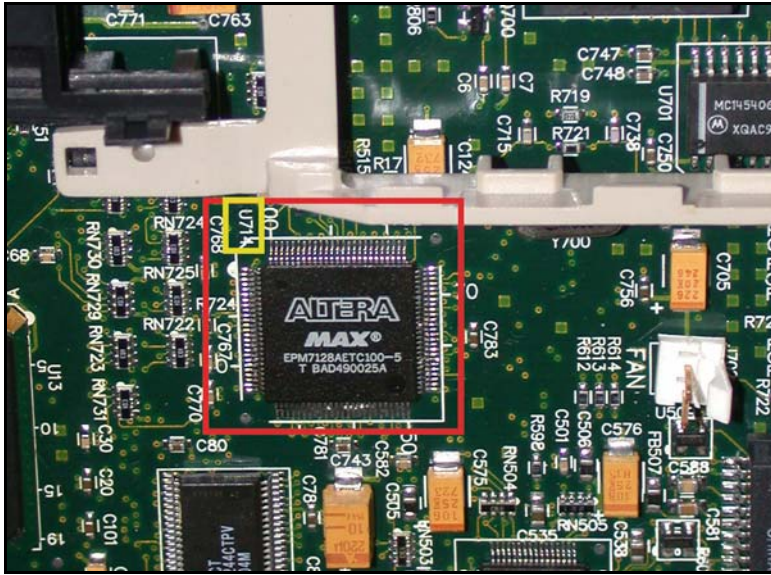
Figure 7. 1721: Non-compliant Altera PLD with Incorrect Speed

Action: Examine the Altera PLD chip at position **U714** on the PCB. Divert Cisco 1721 product that does not use part number **EPM7128AETC100-7**.

Defect 4: Side Chassis – Side- Rear Case Vents Imperfection

Description: On the Cisco 1721, two lines of plastic run horizontally and perpendicular to the vent slots along the sides of the case. These lines continue all the way to the rear of the chassis.

On non-compliant 1721 routers, the two plastic lines end prematurely, not continuing through the final slot at the rear of the casing.
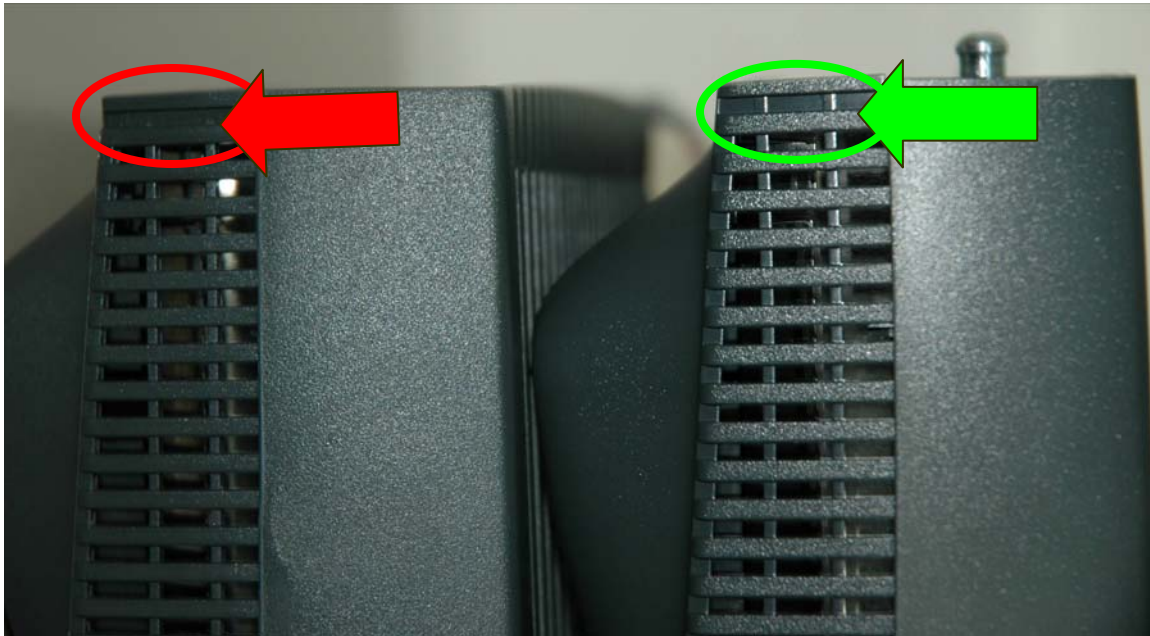
Figure 8. 1721: Non-compliant case (left), and compliant, with lines to end (right)

Action: Examine the casing on the sides of the case to make sure the horizontal lines continue to the rear of the chassis. Divert a unit with case lines that end before the very rear of the chassis.

Defect 5: No Part Number on Fan

Description: On the Cisco 1721, the fan in the top half of the chassis shell has a sticker with a Cisco part number on it. A non-compliant product does not have this sticker, or any other indication of part number, on the fan.

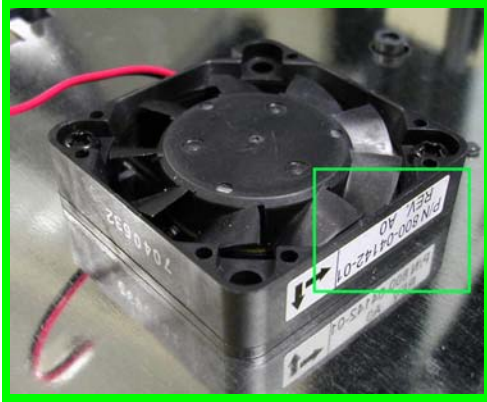**Figure 9. 1721: Non-compliant fan has no part number sticker**

Figure 10. 1721: Fan with correct part number sticker per specification

Action: Divert Cisco 1721 product with no part number on the fan as potential counterfeit.

Defect 6: JTAG test points misspelled as "JTAC"

Description: On Cisco 1721 units, the test points on the PCB are labeled "**JTAG**". The test points are a row of contacts on the PCB at position **J1**, and are completely filled with silver-colored solder on genuine units. Certain non-compliant units have the test point label misspelled "**JTAC**". The test points on an anomalous product are bare copper or incompletely tinned with solder.
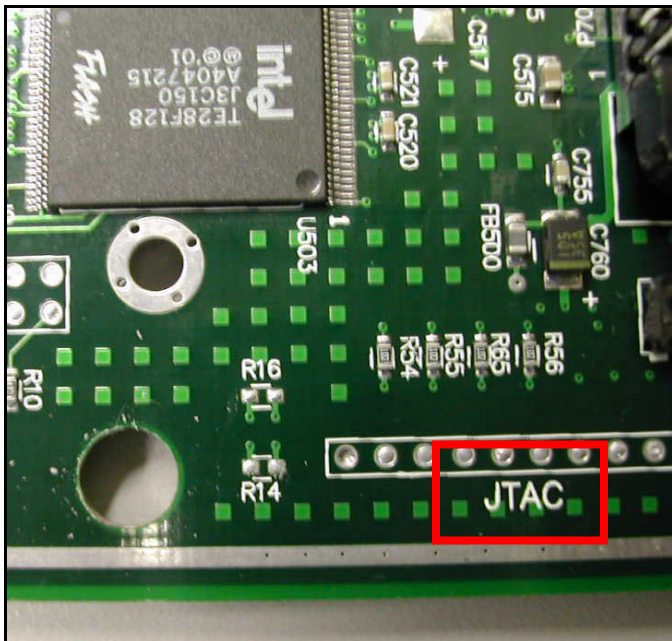

Figure 11. 1721: PCB with test points misspelled "JTAC"

Action: Examine the area around the test point label at position **J1** on the PCB. Divert Cisco 1721 product with test points with incomplete solder, or with the "**JTAC**" label spelling.

Recommendations

Organizations should follow the instructions provided above detailing how to check Cisco routers to determine if they are counterfeit.   Any suspect counterfeit routers should be reported to US-CERT. Final determination as to the status of a router may only be made in coordination with Cisco Systems.

Contact US-CERT

For any questions related to this report, please contact US-CERT at:

> Email: soc@us-cert.gov
> Voice: 1-888-282-0870
> Incident Reporting Form: https://forms.us-cert.gov/report/

Document FAQ

What is a CIIN? A Critical Infrastructure Information Notice (CIIN) is intended to provide warning to US critical infrastructure owners and operators when a particular cyber event or activity has the potential to impact critical infrastructure computing networks.

I see that this document is labeled as UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). Can I distribute this to other people? Per the U//FOUO warning, this document may be shared with personnel who have a valid "need to know." With the case of a CIIN, this is defined as a person or group that has a direct role in securing US critical infrastructure networks. If necessary, please contact US-CERT for clarification or specific distribution inquiries.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.