AUTOMATIC DATA PROCESSING

Software Analysis and Release Standards Report

Cisco ACI Switch – 15.2(5c)

30/Jun/2022

Version 1.1

Cisco Systems, Inc.
Corporate Headquarters
170 West Tasman Drive
San Jose, CA 95134-1706 USA
http://www.cisco.com
Tel: 408 526-4000 Toll Free: 800 553-NETS (6387)
Fax: 408 526-4100

Contents

List of Figures and Tables

About This Software Analysis and Release Standards Report for Cisco ACI Switch– 15.2(5c)

Author	Mohammed Shareef (mosharee)
Change Authority	Customer Experience, Cisco

History

Version No.	Issue Date	Status	Reason for Change
0.1	15-06-2022	Released	Initial draft for review
1.1	30-06-2022	Released	Final Draft

Review

Version	Reviewer's Details	Date
0.1	Prathyusha Bandreddi (pbandred)	15-06-2022
1.0	Sanchita Roy	30-06-2022

1 Introduction

1.1 Preface

The goal of Cisco Customer Experience is to improve AUTOMATIC DATA PROCESSING network stability by proactively identifying potential software bugs. This information can then facilitate software upgrades or operational readiness to remove or reduce the impact of bugs.

1.2 Audience

This document is intended to be used by Cisco Customer Experience (CX) and AUTOMATIC DATA PROCESSING.

1.3 Scope/ Deployment

This Software Analysis and Release Standards Report is intended to document and proactively alert AUTOMATIC DATA PROCESSING of any bug that could result from implementing 15.2(5c) software version on Cisco ACI Switch product family, including potential impact to the AUTOMATIC DATA PROCESSING's network.

2 Executive Summary

2.1 Purpose

The Software Analysis and Release Standards report is intended to provide AUTOMATIC DATA PROCESSING with a software code recommendation for the risk analysis of the currently running software or new software based on a number of requirements including hardware, software, features, performance, availability, and business goals

2.2 Value

The insights from this analysis will help customer proactively identify any risk associated with the selected software release and prepare a plan to mitigate the risk. This in turn will help

- Reduce network downtime and ensure high availability
- Reduce operational and maintenance overhead.

2.3 Recommendations

1. Cisco **recommends** to run **15.2(5c)** software version on **Cisco ACI Switch** devices in the AUTOMATIC DATA PROCESSING network.
2. Cisco will schedule a meeting to walk-through this recommendation with all key stakeholders to ensure understanding.
3. Upon a decision to move forward with code deployment, Cisco recommends a thorough test plan and design / implementation peer review prior to deploying into a production environment.

3 Impact Analysis

Impact analysis is the process of assessing bugs in a software release to identify any potentially impacting bugs based on AUTOMATIC DATA PROCESSING's requirements. A comprehensive Cisco database is searched through the use of an intelligent query for bugs based on customer requirements related to design, risk, security, hardware, software, features, performance, availability requirements, etc.

Note:

- Bugs managed by the Cisco Product Security Incident Response Team (PSIRT) are not included as they are confidential until publicly announced.
- Software bugs identified through software recommendations or Bug Search Tools are not a basis for production SMU requests.
- Some defects might still be investigated so some of these details may change over time or some new defects might get added as well.

A summary of the bugs that are relevant to AUTOMATIC DATA PROCESSING's environment while evaluating the target software version is shown below:

3.1 Impact analysis summary

A summary of the bugs that are relevant to **AUTOMATIC DATA PROCESSING**'s environment while evaluating the target software version is shown below:

Table 1: Summary of Number of Bugs Identified by Customer Severity

Customer Severity	Count
Show Stopper	0
S1	0
S2	0
S3	2
S4	0
S5	0
S6	0
Info-Only	6
Total	7

3.2 Defect Review

3.2.1 Show Stopper Bug Review

No Show Stopper bugs found.

3.2.2 Severity-1 Bug Review

No Severity-1 bugs found.

3.2.3 Severity-2 Bug Review

No Severity-2 bugs found.

3.2.4 Severity-3 Bug Review

Bug ID: CSCwb07205	Severity: 3	Customer Severity: 3	State: Verified
Feature: None	Hardware: None	Platform: None	

Headline	Spine skipping the COOP update after multiple EP move
Impacted Platforms	Cisco Nexus 9000 Series Switches
CX Comments	Note: It is a timing issue and is related to IP moves not mac-based EP moves. There is no known hard value on number of IP moves but in local setup what we have seen is 100+ IP moving continuously for more than 30 min have a potential to cause the issue. This issue has a functional impact. Observed that spine skipped the COOP update after multiple EP (Endpoint) moves. As a result, loss of reachability to an ACI endpoint may occur. This issue is seen when there is a rapid flap of the endpoint IP address that is between different leaf switches. After the endpoint has moved to the new location, traffic from the endpoint IP address is still received on the old leaf switch. Steps to reproduce: 1) EP: 161.113.198.11 originally associated with mac 3c57.3150.0890 on leaf 561 2) During the issue first EP 161.113.198.11 moved from leaf 561 to leaf 701 from mac 3c57.3150.0890 to 0050.569c.aee8. 3) Bounce entry created on leaf 561 as expected. 4) At almost the same time EP got learned back locally on leaf 561 and bounce entry was not created back on node-701 5) Leaf 701 sending COOP update to the spine for the first EP move 6) After EP got learned back locally on leaf 561, it's sending COOP update to spine. The recorded timestamp is older than the COOP update sent by 701 above. 7) Spine skipping the COOP update sent by leaf 561 and as a result, the latest EP coop entry isn't updated on SPINE, and consequently bounce entry does not program on node-701 The is no known workaround available for this issue. On the recovery side, two ways system will recover: a. one hour coop refresh cycle, where the ep will refresh and system recover without any intervention. b. Manual intervention : clear the endpoint on both the leaf using following command "clear system internal epm endpoint " This is an externally found issue with 1 service request. This issue is not fixed in the target release throttle.
Release notes	Symptom: There is a loss of reachability to an ACI endpoint following a move of the endpoint. The new leaf switch has a correct local endpoint entry, but the entry is deleted in COOP on the spine switches.

Bug ID: CSCwb07205	Severity: 3	Customer Severity: 3	State: Verified
Feature: None	Hardware: None	Platform: None	

Traffic from any remote leaf switch that is relying on a spine switch proxy lookup fails as a result. A local endpoint entry may also be present on two separate leaf switches simultaneously.

Conditions:
This issue occurs when there is a rapid flap of the endpoint IP address that is between different leaf switches. After the endpoint has moved to the new location, traffic from the endpoint IP address is still received on the old leaf switch.

Workaround:
There is no workaround to prevent the issue .

On the recovery side , Two ways system will recover .

a. one hour coop refresh cycle , where the ep will refresh and system recover without any intervention .

b. Manual intervention : clear the endpoint on both the leaf using following command
"clear system internal epm endpoint "

Bug ID: CSCwc02860	Severity: 3	Customer Severity: 3	State: Assigned
Feature: EPG	Hardware: None	Platform: None	

Headline	policyelem hap reset when configuring BD/EPG over 500
Impacted Platforms	Cisco Nexus 9000 Series Switches

CX Comments

This issue has an operational impact.

Policyelem crashed when over 500 BD/EPGs (Bridge Domain/Endpoint Groups) are created via REST API and as a result, leaf switches ae reloaded unexpectedly due to policyelem hap reset.

This issue is seen when configuring BD/EPG over 500.
Steps to reproduce:
Configure BD/EPG via REST API.

As a workaround:

1.
Use one PhysDom with 4K vlans for all EPGs:
EPG1 => PhysDom => AEP1 => vlan-pool
EPG2 => PhysDom => AEP2 => vlan-pool

Tested with 600 EPGs.

Number of stpDomFabEncap: 4K

2.

Reduce the number of vlan pool size for each physical domain:
EPG1 => PhysDom1 =>AEP=>vlan-pool1 (100 vlans)
EPG2 => PhysDom2 =>AEP=>vlan-pool2 (100 vlans)

Bug ID: CSCwc02860	Severity: 3	Customer Severity: 3	State: Assigned
Feature: EPG	Hardware: None	Platform: None	
	Tested with 600 EPGs. Number of stpDomFabEncap: 60,000 This is an externally found issue with 1 service request. This issue is under investigation.		
Release notes	Symptom: policyelem crashed when over 500 BD/EPGs are created via REST API. Conditions: Configure BD/EPG over 500 Workaround: None		

3.2.5 Severity-4 Bug Review

No Severity-4 bugs found.

3.2.6 Severity-5 Bug Review

No Severity-5 bugs found.

3.2.7 Severity-6 Bug Review

No Severity-6 bugs found.

3.2.8 Info-Only Bug Review

Bug ID: CSCwa10789	Severity: Info-only	Customer Severity: 2	State: Closed
Feature: ACI_SNMP	Hardware: None	Platform: None	
Headline	SNMPD process multiple crashes leading to hap reset		
Impacted Platforms	Cisco Nexus 9000 Series Switches		
CX Comments	Note: The issue is currently not reproducible at Cisco's end to debug, so, can be in information only. The issue is seen from 2021 and has been seen only in 14.2.x releases till date. This issue has an operational impact. Crashes of the snmpd process may be observed, leading to inconsistent behavior when using SNMP polling. This issue is seen after enabling SNMPD(Simple Network Management Protocol)		

Bug ID: CSCwa10789	Severity: Info-only	Customer Severity: 2	State: Closed
Feature: ACI_SNMP	Hardware: None	Platform: None	

on all the devices in the fabric, Moreover, after 251 snmpd crashes, the switch will reload due to snmpd hap reset and no core is generated for this particular crash instance.

There is no workaround. After the switch crash, the issue is not seen anymore.

This is an externally found issue with 3 service requests. This issue is in closed state.

Release notes

Symptom:
After enabling SNMPD on all the devices in the fabric, crashes of the snmpd process may be observed, leading to an inconsistent behavior when using snmp polling.

Moreover, after 251 snmpd crashes, the switch will reload due to snmpd hap reset.

Issue was observed on 14.2(7f)

Conditions:
No particular conditions identified.

Workaround:
No workaround.

After the switch crash, the issue is not seen anymore.

Further Problem Description:
No core are generated for this particular crash instance.

Bug ID: CSCwa13777	Severity: Info-only	Customer Severity: 2	State: Closed
Feature: ACI_QoS	Hardware: None	Platform: None	

Headline

Customer leaf crashed - sdkhal hap reset

Impacted Platforms

Cisco Nexus 9000 Series Switches

CX Comments

// We can monitor it for RCA, currently no information//

This issue has an operational impact.

Observed that the customer leaf crashed generating a core file in this issue. The device crashed without human intervention generating a core file for sdkhal hap reset. There is no known condition for this issue to occur.

There is no known workaround available.

This is an externally found issue with 3 service requests. The issue is closed.

Release notes

Symptom:
Device crashed without human intervention generating a core file for sdkhal hap reset

Conditions:
TBD

Bug ID: CSCwa13777	Severity: Info-only	Customer Severity: 2	State: Closed
Feature: ACI_QoS	Hardware: None	Platform: None	

Workaround:
TBD

Further Problem Description:
TBD

Bug ID: CSCwb91766	Severity: Info-only	Customer Severity: 3	State: Verified
Feature: L3out,VRF	Hardware: None	Platform: None	

Headline	ACI: Upgrading to 5.2(4) from 4.x can cause /32 static routes to not be installed in FIB
Impacted Platforms	Cisco Nexus 9000 Series Switches
CX Comments	// ADP not using pervasive gateway/, including for information only/ This issue has a functional impact Observed that after upgrading to 5.2(4) /32 static routes stop working. This issue is seen when having /32 static routes on an L3out and the routes also fall in a BD subnet range. The issue is triggered when a static route is added which has supernet same as pervasive gateway, it caused this issue. As a workaround 1. Do not use /32 static route that overlaps with a BD subnet range. 2. Use anything else other than a /32. This is an externally found issue with 1 service request. This issue is not fixed in the target release throttle.
Release notes	Symptom: After upgrading to 5.2(4) /32 static routes stop working Conditions: Have /32 static routes on a L3out and the routes also fall in a BD subnet range Workaround: 1. Do not use /32 static route that overlaps with a BD subnet range 2. Use anything else other then a /32 Further Problem Description: This seems to be done on purpose. A check may have been enabled somewhere past 5.0 to check for this overlap. At least on 5.2(4) there is no fault raised and trouble shooting is difficult.

3.2.9 PBR Defects

Bug ID: CSCwb85467	Severity: Info-only	Customer Severity: 3	State: Resolved
Feature: ACI_IPv6,IP_SLA,PBR,VPC	Hardware: None	Platform: None	

Headline	PBR icmp6 ipsla flaps on one of leaf in the vPC when the number of destinations reaches about 20
Impacted Platforms	Cisco Nexus 9000 Series Switches
CX Comments	The issue has a functional impact. Observed that PBR icmp6 ipsla flaps on one of leaf in the vPC. This issue is seen when the number of destinations reaches about 20. In a vPC environment, icmp6 reply returns to one leaf and the another leaf is notified by udp packet. However, the number of udp packets sent from one leaf is less than the number of icmp6 replies received frequently. Another leaf thinks icmp6 reply has not received and if continue to the same destination for 3 seconds or more ipsla will go down (frequency:1 Multiplier:3) Steps to repro: Increase the number of PBR icmp6 ipsla destinations. There is no known workaround. This is an externally found issue with 1 service request. This issue is not fixed in the target release. Note: It is a baseline issue.
Release notes	Symptom: PBR icmp6 ipsla occasionally flap on one of leaf in the vPC. Conditions: As the number of ipsla destinations increases. seems to occur when it comes to about 20 destinations. This happens in ipv6 and does not appear to occur in ipv4 so far. Workaround: None

Bug ID: CSCwb93059	Severity: Info-only	Customer Severity: 3	State: Resolved
Feature: PBR	Hardware: None	Platform: None	

Headline	Combination of Symmetric PBR and Symmetric Etherchannel hash could cause polarization
Impacted Platforms	Cisco Nexus 9000 Series Switches
CX Comments	// PBR information only// The issue has a functional impact. Observed that polarization could happen depending on the number of PBR destinations and members in the port channel. This issue is seen when Symmetric PBR and Symmetric Etherchannel are used together. Steps to repro: 1. PBR policy has two PBR destinations: PBR-dest1 and PBR-dest2. 2. PBR-dest1 is connected via a port-channel with ethernet 1/1-6. 3. PBR hash option is SIP-only and the Symmetric Etherchannel hash option is also SIP-only. 4. When PBR-dest1 is used, traffic is going through 1/1, 1/3 and 1/5 only, not 1/2, 1/4, or 1/6. If the number of members in the port-channel is an odd number such as 5, 7, etc, this doesn't happen. There is no known workaround available. This is an externally found issue with 1 service request. This issue is not fixed in the target release.

Bug ID: CSCwc04832	Severity: Info-only	Customer Severity: 3	State: Resolved
Feature: PBR,VPC	Hardware: None	Platform: None	

Headline	PBR health-group goes down due to ipsla issues on one side of the vPC leaf
Impacted Platforms	Cisco Nexus 9000 Series Switches
CX Comments	// PBR information only// This issue has a functional impact. Observed that health-group goes down due to ipsla issues on one side of the vPC leaf. The issue is seen on down ipsla in one leaf of VPC. The issue is triggered when the destination got tracked as down when it was being tracked as up by one of the VPC peers and tracked as down by the other. There is no known workaround available. This is an externally found issue with 1 service request. This issue is not fixed in the target release throttle.

Bug ID: CSCwc04832	Severity: Info-only	Customer Severity: 3	State: Resolved
Feature: PBR,VPC	Hardware: None	Platform: None	

Release notes

Symptom:
PBR health-group goes down due to ipsla issues only on one side of the vPC leaf

Conditions:
down ipsla in one leaf of vpc

Workaround:
None

4 Deployment process

Cisco recommends that the AUTOMATIC DATA PROCESSING should test all new code in a lab that mimics the production environment. AUTOMATIC DATA PROCESSING should try to create a lab network that closely simulates the traffic flows and applications that exist in the production network.

Testing may be separated into three parts:

- Proof of concept testing
- Functionality testing
- Limited deployment including online testing

Recommended testing includes:

- **Administration:** Day-to-day moves and changes for addresses and interfaces
- **Management:** Day-to-day network management and trending, SNMP, traps, RMON, syslog, NMS integration, NMS GUI, code upgrade and regression
- **Applications:** Response times and features of a typical user and service can best be performed with a pilot feed from the live network. This could remain in place indefinitely as it is valuable for desktop and server problem recreation.
- **Network Failure Scenarios:** Power, processor, interface and link failures
- **Resiliency Testing:** Convergence, recovery, backup scenarios

After these tests have been carried out to AUTOMATIC DATA PROCESSING's satisfaction, the next step is to deploy the code on one or two network elements in a redundant and non-critical area of the network for two or three weeks. During this period, AUTOMATIC DATA PROCESSING and Cisco Customer Experience monitors the status of these network elements to ensure successful deployment. Customer Experience will work with Cisco Development Engineering to work around or fix any new problems identified.

The code should then be rolled out in a controlled and logical fashion.

Critical problems in new code needs approximately six weeks of field exposure to become visible.

5 Appendix A: Requirements Table

The following tables list all of the software and hardware features considered in this Software Analysis and Release Standards Report. If these requirements change then request a new report.

Hardware

Table 2: Requirements Table – Hardware

Model/Platform	Existing Modules	New Modules
Cisco ACI Switch	APIC model: L2, L3 Spine model: Nexus 9504 SUP-A+ Leaf model: Nexus 93180YC-EX & 93180YC-FX, N9K-C93180YC-FX3 Line cards in case of modular chassis: N9K-C9504-FM-E, N9K-X9732C-EX Optics/SFP	Not provided by the customer

Feature

Table 3: Requirements Table – Features

Existing Features	New Features
Service Graph OSPF Static VMware DVS DHCP IPv6 DHCP PTP SPAN Capabilities – Access Side, Fabric Side, Tenant SPAN - Access Span NTP Intersite L3Out In-Band EPG Tacacs DOM Rogue IP Apps- NIR/NIA/ND Transit Routing Multi-Site BGP PBR VZany BFD	Not provided by the customer

6 Appendix B: References and Resources

Reference/Resource	Link
Release Notes	https://www.cisco.com/c/en/us/support/all-products.html
Cisco Field Notices	http://www.cisco.com/warp/public/tech_tips/index/fn.html
Cisco Security Advisories and Alerts	http://tools.cisco.com/security/center/publicationListing.x
Bug Search Tool	https://bst.cloudapps.cisco.com/bugsearch/
Cisco Feature Navigator	https://cfn.cloudapps.cisco.com/ITDIT/CFN/jsp/index.jsp
Cisco Software Research	https://software.cisco.com/research/home
Cisco Content Hub	https://content.cisco.com/welcome.html

7 Appendix C: Bug State

Term	Definition
Assigned (A)	Bug report is assigned to an engineer, who is then responsible for either resolving the bug or reassigning it. Normally, a development engineering manager assigns a bug report to an engineer who is competent in the area of the problem.
Closed (C)	Bug report is valid, but a conscious decision has been made not to fix it in any release. Normally, a development engineering manager moves a bug report to this state.
Duplicate (D)	Bug report describes the same problem as another bug report or this bug report's problem is resolved by the fix of another bug report.
Forwarded (F)	Bug report is being forwarded to the appropriate project, because it was previously submitted to the wrong project. This state should only be used for transitioning bugs between project types.
Held (H)	A fix to the problem exists, but development engineering work is held up pending information or work from an internal or external source that is outside the direct control of the development team responsible for the bug report. For example, waiting for the customer to test the fix or for required work from an external vendor, etc.
Information required (I)	Holding state for bug reports that are awaiting additional information needed to determine the cause of the problem. This is typically additional information, such as a trace or dump or a more descriptive definition of the problem and symptoms. This state is also used when a diagnostic or special image has been provided to the customer in order to gather more information to continue the analysis. In either case, development engineering cannot make progress until the required information is provided.
Junked (J)	Bug report does not represent a valid bug. The bug report does not describe a problem which requires a change to hardware, software or documentation.
More (M)	Problem described in the bug report is fixed and tested in some, but not all versions in which it is intended to be fixed. Placing a bug report into this state allows the fixed code to be integrated into some releases. The engineer moves the bug report into the Resolved state when the problem is fixed in all versions.
New (N)	New bug report. A bug remains in this state until it is evaluated.
Open (O)	Bug report is actively being worked on by the assigned engineer. Normally, the assigned engineer moves the bug report into this state to indicate that work is in progress.
Postponed (P)	Holding state for a bug report that is not being actively addressed, because the engineering manager or project team has given it a lower

Term	Definition
	priority, and decides to postpone to a later release or phase of the project.
Resolved (R)	Problem described in the bug report is fixed in all release versions where it is TARGETED TO BE FIXED, and all changes have been successfully tested by the developer. Normally, the assigned development engineer moves a bug report into this state.
Unreproducible (U)	Problem cannot be reproduced in the version for which it was reported.
Verified (V)	Fix for the problem has been tested. This is the final resting place for all fixed bug reports that are confirmed to be fixed. Normally, the test engineer moves a bug report into this state.
Waiting (W)	Bug represents an authentic hardware, software or documentation problem that is worthy of engineering attention, but no one inside the direct control of the development team responsible for the bug is available to work on it at this time. W is used when the bug is planned to be fixed in the current release. If a bug is not planned to be fixed until the next release or phase of the project, then use P.

8 Appendix D: Acronym Listing

Term	Definition
CX	Customer Experience
BCS	Business Critical Services
DCP	Delivery Content Portal
GUI	Graphical User Interface
NMS	Network Management System
PID	Product Identification [number]
PSIRT	Product Security Incident Response Team
RMON	Remote Network Monitoring
S	Severity
SEV	Severity
SNMP	Simple Network Management Protocol
Syslog	System log

Document Conventions

Alerts readers to take note. Notes contain helpful suggestions or references to material not covered in the document.

Alerts readers to be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Alerts readers of a situation that could cause bodily injury. They need to be aware of the hazards involved with electrical circuitry and familiarize themselves with standard practices for preventing accidents.

Alerts the reader that they can save time by performing the action described in the paragraph affixed to this icon.

Alerts the reader that the information affixed to this icon will help them solve a problem. The information might not be troubleshooting or even an action, but it could be useful information similar to a Timesaver.

Trademarks and Disclaimers

Document Acceptance

Name		**Name**	
Title		**Title**	
Company		**Company**	
Signature		**Signature**	
Date		**Date**	

Name		**Name**	
Title		**Title**	
Company		**Company**	
Signature		**Signature**	
Date		**Date**	

Name		**Name**	
Title		**Title**	
Company		**Company**	
Signature		**Signature**	
Date		**Date**	