Release Notes for ADC Plugin Version, Release 2.74.gh4.2832

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

ADC P2P Plugin, Release 2.74.gh4.2832 3
New software features 3
Resolved issues 5
Open issues 6
Known issues 6
Compatibility 6
Related resources 7
Legal information 7

© 2026 Cisco and/or its affiliates. All rights reserved.

ADC P2P Plugin, Release 2.74.gh4.2832

This Release Note identifies all changes and issues related to this ADC Plugin Release for the StarOS™ based Application Detection Control (ADC) in-line service, formerly known as Peer-to-Peer Detection.

For more information about the ADC P2P product documentation, see the Related resources section.

New software features

There are no new and enhanced software features introduced in this release.

Enhanced Protocols and Applications Support

These enhancements are added to support new clients/versions for the existing protocols/applications.

Table 1. Enhanced protocols and applications, Release 2.74.gh4.2832

CDETS ID	CDETS Headline/Change Summary
CSCww75562	SSL Server name extension header Fragmentation Issue in Zoom. **Change Summary**: Fragmentation of the SSL SNI header affects Zoom traffic. Detection Percentage: 95.5% Zoom (Android): 7.1.6.41876 Zoom (iOS): 7.1.5
CSCww72539	Improved stun check logic to prevent Instagram, Facebook misclassification to Linkedin **Change Summary**: Instagram and Facebook flows were misclassified as LinkedIn due to an improper STUN check function in LinkedIn. Detection Percentage: 91.51% Linkedin (Android): 4.1.1242 Linkedin (iOS): 9.1.566
CSCww67247	Improve detection for TikTok application. **Change Summary**: Added support for QUIC SNI's in TikTok. Detection Percentage: 99.82% TikTok (Android): 47.0.3 TikTok (iOS): 47.0.0
	Improve detection for AmazonVideo application **Change Summary**: Added support for QUIC SNI's in AmazonVideo. Detection Percentage: 99.61% AmazonVideo (Android): 3.0.470.1047 AmazonVideo (iOS): 10.146.1
	Improve detection for Twitter application. **Change Summary**: Added support for third party flows in Twitter.

© 2026 Cisco and/or its affiliates. All rights reserved.

CDETS ID	CDETS Headline/Change Summary
	Detection Percentage: 94.52% Twitter (Android): 12.22.0-prod.01 Twitter (iOS): 12.23
	Improve detection for Shahid application **Change Summary**: Added support for TLS/QUIC SNI's in Shahid. Detection Percentage: 94.5% Shahid (Android): 8.8.0 Shahid (iOS): 8.7.0
	Improve detection for Clashroyale application **Change Summary**:. Added support for TLS SNI's in Clashroyale. Detection Percentage: 98.23% Clashroyale (Android): 160402002 Clashroyale (iOS): 15.535.29
	Improve detection of Minecraft application. **Change Summary**: Added support for TLS SNI's in Minecraft. Detection Percentage: 98.99% Minecraft (Android): 1.26.52.3 Minecraft (iOS): 26.51
	Improve detection for Discord application. **Change Summary**: Added support for TLS SNI's in Discord. Detection Percentage: 95.4% Discord (Android): 343.12 Discord (iOS): 343
	Improve detection for Nana application. **Change Summary**: Added support for TLS SNI's in Nana. Detection Percentage: 96.02% Nana (Android): 37.8.6 Nana (iOS): 37.8.2
	Improve detection for ParamountPlus application. **Change Summary**: Added support for TLS SNI's in ParamountPlus. Detection Percentage: 96.3% ParamountPlus (Android): 16.19.1 ParamountPlus (iOS): 15.25.0
CSCww75087	Improve detection for Telegram application.

© 2026 Cisco and/or its affiliates. All rights reserved.

CDETS ID	CDETS Headline/Change Summary
	Change Summary: Added support for new encrypted TCP flow. Detection Percentage: 97.42% Telegram (Android): 12.10.1 Telegram (iOS): 12.9.3
CSCww72869	Implement QUIC/TCP SNI support and SSL fragmentation detection for Google maps traffic. **Change Summary**: Improved Google Maps detection with QUIC/TLS SNI and SSL fragmentation support. Detection Percentage: 71.13% Google Maps (Android): 26.35.03.969485213 Google Maps (iOS): 26.33.1
CSCww67188	Roblox support for QUIC fragmentation with addition of a new string. **Change Summary**: Added QUIC fragmentation support and a new QUIC string to improve Roblox traffic classification. Detection Percentage: 92.47% Roblox (Android): 2.736.1408 Roblox (iOS): 2.735.1135
CSCww75167	Improve Detection for the PubG TCP flows. **Change Summary**: New version of PubG application TCP flows are not classified as PubG. Detection Percentage: 98.92% PubG (Android): 4.6.0 PubG (iOS): 4.6.0
CSCww72793	Added QUIC and TLS fragmentation support with new QUIC string for improved traffic classification **Change Summary**: Added QUIC and TLS fragmentation support and a new QUIC string to improve Jawwy TV traffic classification. Detection Percentage: 97.77% Jawwy TV (Android): 10.2.0 Jawwy TV (iOS): 10.2.1

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug number> site:cisco.com.

© 2026 Cisco and/or its affiliates. All rights reserved.

Table 2. Resolved issues for ADC P2P Plugin, Release 2.74.gh4.2832

Bug ID	Description	Product Found
CSCwv96810	P2P offload Difference Observed with TLS QUIC Fragment Detection Enabled vs Disabled	pdn-gw
CSCwu66329	Code Optimization: Improving TLS certificate header processing	pdn-gw
CSCww02096	Enhanced decoding of QUIC transport parameter length in QUIC CH header	pdn-gw
CSCwv92274	Code Fix and Optimizations in CSV file generated in PCAP processing	pdn-gw
CSCww78110	Improved detection for Jaco application	pdn-gw

Open issues

There are no open issues in this specific software release.

Known issues

This section describes the known issue that may occur during the upgrade of the ADC plugin image.

Install and Upgrade Notes

This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Compatibility

This section provides compatibility information about the P2P package version, and the hardware and software requirements for the Legacy Gateway and CUPS software release.

Compatible Release package version

Table 3. Release package version information

ADC release	StarOS compatible versions
2.74.gh4.2832	StarOS-2025.04.gh0 /StarOS-2026.04.gh1 /StarOS-2026.02.gah0 or later releases

Note: For any StarOS prior to above mentioned, ensure that you use p2p version 2.74.h7.2683 or an earlier version released before July 2025.

ADC plugin version numbering system

This section explains the version-numbering scheme for ADC Plugin releases running on the ASR 5x00 or Cisco Virtualized Packet Core platform. The version numbering is different for the ADC Plugin release as this release is independent of StarOS software releases.

The fields of the version number as reflected in the ADC Plugin are in the form of INTERFACE.MAJOR.BUILD (e.g., 1.140.514).

- The INTERFACE number indicates the identifier between ASR5x00 and Plugin. This number indicates backward compatibility and only increments when a change will introduce a compatibility issue. This field may increment by '1' when necessary.

© 2026 Cisco and/or its affiliates. All rights reserved.

- The MAJOR version number indicates a contiguous sequential number that represents incremental changes between releases. This number increments by ‘1’ for each plugin release.
- The BUILD version number indicates the build number that increments with each new build. This is a unique, sequential number across all ADC builds.

Related resources

This table provides key resources and links to the support information and essential documentation for StarOS and ADC products.

Table 4. Related resources and additional information

Resource	Link
Cisco ADC Administration documentation	ADC Administration Guide
Cisco Command line Interface documentation	Command Line Interface Reference
Service request and additional information	Cisco Support

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved.