Release Notes for Cisco Catalyst ESS9300 Embedded Series Switches, Release 26.1.x

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

Contents

Cisco Catalyst ESS9300 Embedded Series Switches, Release 26.1.x 3
New hardware features 4
Change in behavior 4
Resolved issues 5
Open issues 5
Known issues 6
Compatibility 6
Supported software packages 7
Related resources 8
Legal information 9

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

Cisco Catalyst ESS9300 Embedded Series Switches, Release 26.1.x

This document provides release information for the Cisco Catalyst ESS9300 Embedded series switch. It is a Small Form Factor Ruggedized 10 GigE Embedded platform for tactical, outdoor, and mobile environments. The compact design simplifies integration and offers the system integrator the ability to use the Cisco Catalyst ESS-9300-8X16T of the Curtiss-Wright VPX3-623 Embedded Series Switch in a wide variety of applications. It consists of one switch card. Cooling plates are not included. The system integrator must provide an appropriate thermal solution. Thermal power of the switch is 35 watts.

New software features

This section provides a brief description of the new software features introduced in the Cisco IOS XE Release 26.1.x.

IOS XE 26.1.2

There are no new software features in Cisco IOS XE Release 26.1.2.

IOS XE 26.1.1

Table 1. New software features release 26.1.1

Product Impact	Feature	Description
Security	Resilient Infrastructure	As part of the ongoing commitment to network security, this Cisco IOS XE release introduces secure alternatives to legacy commands. These updates are designed to mitigate potential risks and assist in establishing a more robust and secure operational baseline. The identified insecure commands are categorized as: • Line transport: Updates to secure remote access methods. • Device server configuration: Hardening of server-side settings. • File transfer protocols: Transitioning to encrypted transfer methods. • SNMP: Enhancements to secure management traffic. • Passwords: Strengthening authentication and credential management. • Miscellaneous: General security improvements for various system functions. The **show system insecure configuration** command introduced in Cisco IOS XE release 17.18.2 lists all insecure commands configured on the device. For all detected insecure configurations during device boot or upgrade, error messages are displayed. In Cisco IOS XE release 26.1.1, all insecure CLI commands are blocked by default to strengthen your network infrastructure. If your environment requires the use of a legacy command, you must enable the **system mode insecure** command in global configuration mode. • Recommendation: Do not use insecure mode. This mode is temporary and will be removed in a future Cisco IOS XE release. Identify and replace all insecure commands with their secure alternatives. • Upgrade behavior: If you upgrade to Cisco IOS XE release 26.1.1 with insecure commands already present in the running configuration, the **system mode insecure** command is automatically added to your configuration to prevent service disruption. For more information, refer to Resilient Infrastructure IOS XE Security Warnings Reference

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

Product Impact	Feature	Description
Upgrade	PROFINET system redundancy	This feature enables Cisco Industrial Ethernet (IE) switches to interoperate with existing high-availability systems by providing robust controller failover using PROFINET S2 controller redundancy mode. It aims to minimize potential issues and downtime in the event of network or controller failures.
Software Reliability	Read-only PROFINET	This feature enhances device security and network flexibility by setting Discovery and Configuration Protocol (DCP) operations to read-only mode. It safeguards the IP address, gateway, and device name from modifications, protects essential network settings to prevent unexpected connectivity loss, and remains compatible with LLDP, SNMP, and CDP. Additionally, it enables devices to carry out identification and basic network discovery.

New hardware features

This section provides a brief description of the new hardware features introduced in Cisco IOS XE Release 26.1.x

IOS XE 26.1.2

There are no new hardware features in Cisco IOS XE Release 26.1.2

IOS XE 26.1.1

There are no new hardware features in this Cisco IOS XE Release 26.1.1

Change in behavior

Syslog warning on reload for SSH Hostkeys

After a device reload, a syslog warning may appear indicating insufficient key length, even when a strong RSA or EC key is already configured.

Note:

- If the syslog warning message displays ***crypto key generate rsa modulus <modulus-size> label <label-name>,*** then the *<modulus-size>* and *<label-name>* represent the actual modulus size and label configured on the device.
- The SSH keypair association configuration is done using the command: **ip ssh ec|rsa <**keypair-name**>**, where *<keypair-name>* corresponds to the keypair name configured on the device.

Example warnings:

RSA

Warning Observed: INSECURE DYNAMIC WARNING - Module: SSH.

Command: crypto key generate rsa modulus <modulus-size> label <label-name>.

Reason: An SSH hostkey has been provisioned on the device with insufficient key length.

Remediation: Provision an SSH RSA hostkey with minimum modulus size of 3072 bits for enhanced security.

Sub mode: exec.

Parent CLI: Not Applicable.

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

EC

Warning Observed: INSECURE DYNAMIC WARNING - Module: SSH.

Command: crypto key generate ec keysize <modulus-size> label <label-name>.

Reason: An SSH hostkey has been provisioned on the device with insufficient key length.

Remediation: Provision an SSH hostkey with minimum modulus size of 256 bits for enhanced security.

Sub mode: exec.

Parent CLI: Not Applicable.

If you have already configured a strong key and associated it using **ip ssh ec|rsa <keypair-name>**, you can ignore this warning during boot. The configured SSH keypair association is applied after the boot process, and SSH then uses the correct key for secure connections once the configuration is active.

Resolved issues

This section lists resolved issues in Cisco IOS XE Release 26.1.x.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID in Cisco Bug Search Tool.

IOS XE 26.1.2

Table 2. Resolved issues in release 26.1.2

Bug ID	Description
CSCwu29126	IE9300 - ALT port failing to block traffic, causing network loops in REP ring

IOS XE 26.1.1

Table 3. Resolved issues in release 26.1.1

Bug ID	Description
CSCwr77016	Cisco IOS XE Software for Cisco Catalyst and Rugged Series Switches Secure Boot Bypass Vulnerability

Open issues

This section lists the open issues in Cisco IOS XE Release 26.1.x.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

IOS XE 26.1.2

No customer-impacting bugs were identified in this release.

IOS XE 26.1.1

No customer-impacting bugs were identified in this release.

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

Known issues

This section lists known issues in Cisco IOS XE Release 26.1.x

IOS XE 26.1.2

There are no known issues in this release.

IOS XE 26.1.1

There are no known issues in this release.

Compatibility

SSH algorithms for common criteria certification limitation

Starting from Cisco IOS XE Release 17.10, the following Key Exchange and MAC algorithms are removed from the default list:

- Key Exchange algorithm:
  - diffie-hellman-group14-sha1
- MAC algorithms:
  - hmac-sha1
  - hmac-sha2-256
  - hmac-sha2-512

Note: Use the **ip ssh server algorithm kex** command to configure the Key Exchange algorithm and the **ip ssh server algorithm mac** command to configure the MAC algorithms.

Table 4. Hardware feature mapping between Cisco ESS 9300-10X-E and Cisco ESS-9300-8X16T of the Curtiss-Wright VPX3-623:

Category	Feature	Cisco ESS-9300-10X-E	Cisco ESS-9300-8X16T of the Curtiss-Wright VPX3-623
Hardware	Single board	Yes	Yes
	Small form-factor with mezzanine card	Supported with 4.595 in.(H) x 2.904 in.(W)	Supported with 5.1 in.(H) x 2.9 in.(W)
	Ethernet management port	Optional	Not supported
	Optical ports	10X10 GE optical ports with Enhanced Small Form-Factor Pluggable (SFP+).	• 8x10GE interfaces. By default, 2x10GE interfaces are configured in backplane mode and 6x10GE interfaces in the optical mode. • 10X1 GE Copper ports
	RS-232 console	Supported	Supported
	USB console	Supported	Not supported
	Common +3.3VDC and +5VDC power inputs	Supported	Supported

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

Category	Feature	Cisco ESS-9300-10X-E	Cisco ESS-9300-8X16T of the Curtiss-Wright VPX3-623
	Low power—35 W (typical)	Supported	Supported
	ARM Quad-Core A53	Supported	Supported
	Alarms	• Two—input • One— output	• Four—input • One— output
	4 GB of DDR4 DRAM with ECC	Supported	Supported
	Eight GB onboard eMMC flash storage (2.5 GB usable space).	Supported	Supported
	Input/Output	• SD card slot • Power input • RJ-45 (RS-232) console • Micro-USB console • USB-A host port	• Power input • RJ-45 (RS-232) console • USB-A host port
Software	IOS XE, Network Essentials and Network Advantage	Supported	Supported
Industrial temperature	-40° C to +85° C	Supported	Supported

Refer to Cisco IOS XE Migration Guide for IIoT Switches for the latest information about upgrading and downgrading switch software for Cisco Catalyst ESS9300 Series Switches.

Supported software packages

Finding the software version

- The package files for Cisco IOS XE software can be found on the system board's internal flash memory device (flash:) or an external USB, depending on the platform configuration.
- Use the **show version** privileged EXEC to display the software version running on the switch. The model name displayed at the end of the output reflects the factory configuration and does not change after software license upgrades.
- Use the **dir filesystem:** privileged EXEC command to view the names and versions of software images stored in flash memory.

Software images for Cisco IOS XE 26.1.x

This table provides the filename for the IOS XE 26.1.x software image for Cisco Catalyst ESS-9300-8X16T of the Curtiss-Wright VPX3-623 Embedded Series Switches.

Table 5. Software package for release 26.1.x

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

Release	Image Type	Filename	Switch Models
Cisco IOS XE 26.1.2	Universal	ie9k_iosxe.26.01.02.SPA.bin	Cisco Catalyst ESS-9300-10X-E Cisco Catalyst ESS-9300-8X16T of the Curtiss-Wright VPX3-623 Embedded Series Switches
Cisco IOS XE 26.1.1	Universal	ie9k_iosxe.26.01.01.SPA.bin	Cisco Catalyst ESS-9300-10X-E Cisco Catalyst ESS-9300-8X16T of the Curtiss-Wright VPX3-623 Embedded Series Switches

Software installation options

This table lists the options for the **install** command for the Cisco Catalyst ESS-9300-8X16T of the Curtiss-Wright VPX3-623 Embedded Series Switch.

To install and activate the specified file, and to commit changes to be persistent across reloads, enter the following command: **install add file filename [activate commit]**

Table 6. Summary of software installation commands for install mode

Option	Description
abort	Abort the current install operation.
activate	Activate an installed package.
add	Install a package file to the system.
auto-abort-timer	Install auto-abort-timer.
autoupgrade	Initiate software auto-upgrade on all incompatible switches.
commit	Commit the changes to the load path.
deactivate	Deactivate an install package.
label	Add a label name to any installation point.
remove	Remove installed packages.
rollback	Rollback to a previous installation point.

Related resources

Table 7. Additional references for Cisco Catalyst ESS-9300-8X16T of the Curtiss-Wright VPX3-623 Embedded Series Switches

Document	Description
Cisco IOS XE	Provides information about Cisco IOS XE

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

Document	Description
Cisco Catalyst ESS-9300-8X16T of the CURTISS-WRIGHT VPX3-623 Embedded Series Switches	Provides information about Cisco Catalyst ESS-9300-8X16T of the CURTISS-WRIGHT VPX3-623 Embedded Series Switches
Cisco Validated Designs	Provides information about Cisco-Validated Designs.
Cisco MIB Locator	Provides tools for locating and downloading MIBs.
Cisco Profile Manager	Provides timely and relevant information from Cisco.
Cisco Services	Provides the business outcomes and technical support services needed to maximize the value of your Cisco technologies.
Cisco Support	You can submit a service request here.
Cisco DevNet	Enables you to discover and browse secure, validated, enterprise-class applications, products, solutions, and services.
Cisco Press	Provides general networking, training, and certification titles.
Cisco Warranty Finder	Provides warranty information for a specific product or product family.
Cisco Support Community	You can ask and answer questions, share suggestions, and collaborate with your peers.
Cisco TAC	Provides most up-to-date, detailed troubleshooting information. Go to Product Support and select your product from the list or enter the name of your product. Look under Troubleshoot and Alerts, to find information for the problem that you are experiencing.
Cisco Feature Navigator	Provides platform support details and license level information for features. The CFN also has a tab that provides a MIB Locator.
Documentation Feedback	To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Licensing

This section provides information about the licensing packages for features available on the Cisco Catalyst ESS-9300-8X16T of the Curtiss-Wright VPX3-623 Embedded Series Switch. For information about the licensing packages for features available on Cisco Catalyst ESS9300 Embedded Series Switch, see Licensing on the Cisco Catalyst IE9300 Series Switches.

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.

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