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

Contents

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. There is no cooling plates sold with it. It is up to the system integrator to design a thermal solution with it. Thermal power of the switch is 35 Watts.

Cisco Catalyst ESS9300 Embedded Series Switch

The Catalyst ESS9300 Embedded Series Switch is a ruggedized 10G embedded platform that is designed for embedded applications for tactical, outdoor, and mobile installations requiring low power, small size, and ruggedization.

New software features

This section provides a brief description of the new software features introduced in this release.

IOS-XE 26.1.1

Table 1. New software features in release 26.1.1

Product Impact	Feature	Description
Security	Resilient Infrastructure	As part of the ongoing commitment to network security, this 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 17.18.2 release 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 26.1.1 release, 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 release. Identify and replace all insecure commands with their secure alternatives. • Upgrade behavior: If you upgrade to Cisco IOS XE 26.1.1 release 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
Upgrade	PROFINET system redundancy	This feature enables Cisco Industrial Ethernet (IE) switches to interoperate with existing high available 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. Software Reliability

New hardware features

This section provides a brief description of the new hardware features introduced in this release.

IOS-XE 26.1.1

There are no new hardware features introduced in this release.

Change in behavior

Syslog Warning on Reload for SSH Hostkeys: After a device reload, you may observe a syslog warning indicating insufficient key length for SSH hostkeys, even if a strong RSA or EC key is configured.

Note:

- In the syslog warning message "*crypto key generate rsa modulus <modulus-size> label <label-name>",* 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:

- 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: Please provision an SSH RSA hostkey with minimum modulus size of 3072 bits for enhanced security,

  Submode: exec,

  Parent CLI: Not Applicable.

- 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: Please provision an SSH RSA hostkey with minimum modulus size of 384 bits for enhanced security,

  Submode: exec,

  Parent CLI: Not Applicable.

Ignore these warnings if you have already configured a strong key. The system applies the SSH keypair association (**ip ssh ec/rsa** *keypair-name*) after the boot process.

Once this configuration is active, SSH will use the correct key for secure connections.

Notice of changes introduced in the Cisco IOS-XE 17.18.2 release and beyond

Cisco is committed to safeguarding our products and customer networks against increasingly sophisticated threat actors. As computing power and the threat landscape have evolved, some features and protocols currently in use have become vulnerable to attack. While more secure alternatives are now available, legacy protocols may still be in use in some environments.

To improve network security, reduce the attack surface, and protect sensitive data, Cisco will begin phasing out legacy and insecure features and protocols, encouraging customers to transition to more secure alternatives. This process will be gradual and designed to minimize operational impact. The first phase began with the Cisco IOS-XE 17.18 release train. This is part of a broader initiative to make Cisco products more secure by default and secure by design.

Starting with the Cisco IOS-XE 17.18.2 release and in future releases, Cisco software displays warning messages when configuring features or protocols that do not provide sufficient security such as those transmitting sensitive data without encryption or using outdated encryption mechanisms. Warnings also appear when security best practices are not followed, along with suggestions for secure alternatives.

This list is subject to change, but the following is a list of features and protocols that generates warnings in releases beyond the version Cisco IOS-XE 17.18.1. Release notes for each release describes the exact changes for that release.

- **Plain-text and weak credential storage:** Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files.
  *Recommendation***:** Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-SHA-256) or Type 9 (Scrypt) for non-reversible credentials.
- **SSHv1**
  Recommendation: Use SSHv2.
- **SNMPv1 and SNMPv2, or SNMPv3 without authentication and encryption**
  Recommendation: Use SNMPv3 with authentication and encryption (authPriv).
- **MD5 (authentication) and 3DES (encryption) in SNMPv3**
  Recommendation: Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption.
- **IP source routing based on IP header options**
  Recommendation: Do not use this legacy feature.
- **TLS 1.0 and TLS 1.1**
  Recommendation: Use TLS 1.2 or later.
- **TLS ciphers using SHA1 for digital signatures**
  Recommendation: Use ciphers with SHA256 or stronger digital signatures.
- **HTTP**
  Recommendation: Use HTTPS.
- **Telnet**
  Recommendation: Use SSH for remote access.

- **FTP and TFTP**
  Recommendation: Use SFTP or HTTPS for file transfers.
- **On-Demand Routing (ODR)**
  Recommendation: Use a standard routing protocol in place of CDP-based routing information exchange.
- **BootP server**
  Recommendation: Use DHCP or secure boot features such as Secure ZTP.
- **TCP and UDP small servers (echo, chargen, discard, daytime)**
  Recommendation: Do not use these services on network devices.
- **IP finger**
  Recommendation: Do not use this protocol on network devices.
- **NTP control messages**
  Recommendation: Do not use this feature.
- **TACACS+ using pre-shared keys and MD5**
  Recommendation: Use TACACS+ over TLS 1.3, introduced in release Cisco IOS-XE 17.18.1.

Cisco is committed to supporting customers through this transition. Subsequent releases in the Cisco IOS-XE 17.18 train continues to support these features but displays warnings if they are used. Future release trains may impose additional restrictions on these features which will be communicated through release notes.

The changes introduced in 17.18 persist in 26.1.x and later versions.

Resolved issues

This section lists the resolved issues for this release.

IOS-XE 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 this specific software release.

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 26.1.1

There are no open issues in this release.

Known issues

This section lists the known issues in this specific software 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 You can 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 2. 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
	Low power—35W (typical)	Supported	Supported

Category	Feature	Cisco ESS-9300-10X-E	Cisco ESS-9300-8X16T of the Curtiss-Wright VPX3-623
	ARM Quad-Core A53	Supported	Supported
	Alarms	• Two–input • One– output	• Four–input • One– output
	4GB DDR4 DRAM with ECC	Supported	Supported
	Eight GB onboard eMMC flash storage (2.5 GB usable space).	Supported	Supported
	Input/Output	• SD-cards socket • 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, Release 17.18.1.

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 device configuration.
- You can use the show version privileged EXEC command to see the software version that is running on your switch.

Note: Although the show version output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the dir filesystem: privileged EXEC command to see the names and versions of other software images that you might have 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 3. Software package for release 26.1.x

Release	Image Type	Filename	Switch Models
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 4. Summary of software installation commands for install mode

Bug ID	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 5. 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
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 Design documents	Provides Cisco validated designs

Document	Description
Cisco MIB Locator	Provides locating and downloading MIBs
Cisco Profile Manager	To receive timely, relevant information from Cisco, sign up here
Cisco Services	Provides the business impact you're looking for with the technologies
Cisco Support	You can submit a service request here
Cisco DevNet	To discover and browse secure, validated enterprise-class apps, products, solutions, and services
Cisco Press	To obtain general networking, training, and certification titles visit here
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.

Network Essentials and Network Advantage licenses are available for:

- Cisco ESS-9300-10X-E starting with release 17.10.1.
- Cisco ESS-9300-8X16T on Curtiss-Wright VPX3-623 starting with release 17.17.1.

License levels

The software features available on Cisco Catalyst ESS-9300-8X16T of the CURTISS-WRIGHT VPX3-623 Embedded Series
switches fall under these base or add-on license levels.

Base licenses

- Network Essentials
- Network Advantage: Includes features available with the Network Essentials license and more.

Add-on licenses

Add-on licenses require a Network Essentials or Network Advantage as a prerequisite. The features available with add-on license levels provide Cisco innovations on the switch, and on the Cisco Catalyst Center.

- Catalyst Center DNA Essentials

- Catalyst Center DNA Advantage: Includes features available with the Catalyst Center DNA Essentials license and more.

Smart licensing using policy

Smart Licensing Using Policy, which is an enhanced version of Smart Licensing, is the default and the only supported method to manage licenses.

Smart Licensing using Policy provides a licensing solution that does not interrupt the operations of your network. Instead, it enables a compliance relationship to account for the hardware and software licenses you purchase and use.

With this licensing model, you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. Only export-controlled and enforced licenses require Cisco authorization *before* use. License usage is recorded on your device with timestamps, and the required workflows can be completed later.

Multiple options are available for license usage reporting – this depends on the topology you implement. You can use the Cisco Smart Licensing Utility (CSLU) Windows application, or report usage information directly to Cisco Smart Software Manager (CSSM). A provision for offline reporting for air-gapped networks, where you download usage information and upload to CSSM, is also available.

Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to this release.

By default, your Smart Account and Virtual Account in CSSM is enabled for Smart Licensing Using Policy.

Legal information