Release Notes for Cisco IE3500 Series Switches, Release 26.1.x

Contents

Cisco IE3500 Series Switches, Release 26.1.x

This document provides release information for the Cisco Industrial Ethernet (IE) switches.

Cisco IE3500/IE3505 Series Switches

These are ruggedized switching platforms and provides superior bandwidth and high-PoE power with proven Cisco IOS-XE Software for industrial environments. They are hardened to withstand temperatures ranging from freezing cold to extreme heat (-40°C to +75°C or -40°F to 167°F), as well as severe shock and vibration.

The IE3500 switch is designed to cater deployments where hardened products are required, including factory automation, smart cities, energy and process control, Intelligent Transportation Systems (ITS), energy production sites, smart city programs, and mining. They bring improved scale performance, built-in security feature set, and simplified management options for the switch. For more information, refer to the Datasheet.

Cisco IE3500H/IE3505H Series Switches

These are the next-generation managed IP67 switches powered by Cisco IOS-XE and are ideal for deployment in the harshest environments. They are IP67-rated for water and dust resistance and are hardened to withstand temperatures ranging from freezing cold to extreme heat (-40°C to +75°C or -40°F to 167°F), as well as severe shock and vibration.

These switches are available with up to 24 ports. Fast Ethernet is supported through Fast Ethernet PIDs, and 1G PIDs can also be configured to operate at 100M speed. For a list of supported SFPs, refer the Datasheet. These switches can be wall-mounted and deployed without a housing cabinet. They offer a power budget of 240W, and supports Power over Ethernet (PoE), PoE+, and Universal Power over Ethernet (UPOE) at 60W.

These switches are equipped with advanced network-based security, segmentation, and visibility features for the most demanding industrial environments. They extend the power of intent-based networking to the harshest Internet of Things (IoT) edge, with use cases in industries such as mining, railways, and manufacturing. The switches can be wall mounted and deployed without a housing cabinet. For more information, refer to the Datasheet.

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.

Product Impact	Feature	Description
		▪ 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	Frame Preemption with IEEE 802.1Qbu	This feature provides a low-latency mechanism for high-priority frames by allowing the suspension of non-critical frames for critical ones. It helps achieve low latency and low jitter for real-time control networks, effectively extending QoS capabilities. When high-priority frames are transmitted, the preempted non-critical frame resumes transmission for multiple splits.
	Media Redundancy Client	This feature enables configuring Cisco switches as Media Redundancy Clients (MRC) within an MRP ring, acting as regular ring participants that forwards traffic and continuously monitor link status, reporting any failures to the ring manager (MRM). This approach enhances network resiliency and simplifies deployment, supporting rapid failover and compliance with industrial certification requirements.
	PTP over MACsec	This feature allows highly accurate time synchronization between devices, even when MACsec encrypts Ethernet traffic for security. This ensures industrial, utility, or automation networks can maintain precise timing and robust data protection on the same infrastructure.
	HSR-HSR QuadBox	This feature enables you to interconnect two distinct High-availability Seamless Redundancy (HSR) rings, providing continuous, fault-tolerant communication between them. This capability is crucial in industrial and critical infrastructure environments where zero packet loss and high network availability are paramount. It allows for robust network segmentation and enhanced resilience on IE3505 and IE3505H platforms.
Ease of Use	Industrial Asset Discovery	Industrial Asset Discovery feature automatically identifies, and catalogs directly connected industrial devices without impacting network performance. This feature also exports inventory data to a syslog server in JSON format, streamlining asset tracking, and security enforcement.
	Migration to Meraki Managed Dashboard	Cisco Industrial Ethernet IE35xx series switches support cloud management mode, enabling centralized control through the Meraki dashboard. This functionality supports zero-touch provisioning and

Product Impact	Feature	Description
		cloud-based management for streamlined monitoring and configuration. Additionally, it includes access to a Local Status Page (LSP) to facilitate troubleshooting and setup in environments without DHCP.
Ease of use and ease of setup	REP Segment-ID auto-discovery	REP Segment ID Auto-Discovery automates the configuration of Resilient Ethernet Protocol (REP) Segment IDs using CDP. This feature reduces manual effort and prevents mismatches for both standard REP and REP Fast protocols, making it easier to add switches to existing segments or create new daisy-chain segments.
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.

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

To mitigate potential CRC errors on the Cisco IE3105 platform following a device reload, ensure that auto negotiation settings are consistent across both ends of the link (either enabled or disabled on both sides). We also recommend either replacing the **speed auto 100** command with **speed 100 duplex full** or configuring **speed auto 100** at both ends.

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 issues resolved in this 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.

IOS-XE 26.1.1

Table 2. 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 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

Table 3. Open issues in release 26.1.1

Bug ID	Description
CSCwt56767	SWCSTRATIX-8328 S5200: Interface link details and PRP shows down when the interface is actually UP

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.

Supported hardware

This section lists the hardware support information.

Table 4. Supported IE3500 SKUs

PID	Uplink Ports			Downlink Ports		
	Type	Ports	Interface name	Type	Ports	Interface name
IE-3500-8T3S	SFP/SFP+	3	Gigabit Ethernet 1/1-3	Copper	8	Gigabit Ethernet 1/4-11
IE-3500-8P3S						
IE-3505-8T3S						

PID	Uplink Ports			Downlink Ports		
	Type	Ports	Interface name	Type	Ports	Interface name
IE-3505-8P3S						
IE-3500-8U3X			TenGigabit Ethernet 1/1-3			
IE-3500-8T3X						

Table 5. Supported IE3500H SKUs

System	PIDs	SW	Uplinks	Downlinks	Data Path FPGA	PoE	Alternate PIDs (TAA and COO)
All Gig Copper	IE-3500H-8T	Network Essentials or Network Advantage	4x1G Copper	4x1G Copper	No	No	none
	IE-3500H-16T			12x1G Copper			none
	IE-3500H-24T			20x1G Copper			
Mixed Gig/GE Copper	IE-3500H-12FT4T			12xFE Copper	No	No	none
	IE-3500H-20FT4T			20xFE Copper			
Advanced Copper	IE-3505H-16T			12x1G Copper	Yes	No	none
POE	IE-3500H-14P2T		2x1G Copper	14x1G Copper	No	Yes	none
	IE-3500H-12P2MU2X		2x10G SFP	12x1G POE and 2xMGig UPOE			

Supported expansion modules

Table 6. Supported expansion modules

PID	Downlink Ports		
	Type	Ports	Interface name
IEM-3500-16P	Copper RJ45	16 PoE	Gigabit Ethernet 2/1-16

PID	Downlink Ports		
	Type	Ports	Interface name
IEM-3500-16T		16	Gigabit Ethernet 2/1-16
IEM-3500-8P		8 PoE	Gigabit Ethernet 2/1-8
IEM-3500-8T		8	Gigabit Ethernet 2/1-8
IEM-3500-4MU		4 PoE	Gigabit Ethernet 2/1-4
IEM-3500-8S	SFP	8	Gigabit Ethernet 2/1-8
IEM-3500-14T2S	Copper RJ45/ SFP	Copper RJ45: 14 SFP: 2	Gigabit Ethernet 2/1-16
IEM-3500-6T2S		Copper RJ45: 6 SFP: 2	Gigabit Ethernet 2/1-8

Web UI system requirements

The WebUI is a web browser-based switch management tool that runs on the switch. The following subsections list the hardware and software required to access the WebUI.

Minimum hardware requirements

Table 7. Minimum hardware requirements

Processor Speed	DRAM	Number of colors	Resolution
233 MHz minimum We recommend 1 GHz	512 MB We recommend 1 GB DRAM	256	1280 x 800 or higher

Operating systems

- Windows 10 or later
- Mac OS X 10.9.5 or later

Browsers

- Google Chrome: Version 59 or later (On Windows and Mac)
- Microsoft Edge
- Mozilla Firefox: Version 54 or later (On Windows and Mac)
- Safari: Version 10 or later (On Mac)

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.

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 file names for the IOS-XE 26.1.x software images for Cisco Catalyst IE3500 Series Switches.

Table 8. Software package for release 26.1.x

Release	Image Type	Platform	File Name
Cisco IOS-XE 26.1.1	Universal	IE3500, IE3505, IE3500H and IE3505H	ie35xx-universalk9.26.01.01.SPA.bin

Automatic boot loader upgrade

When you upgrade from the existing release on your switch to a later or newer release for the first time, the boot loader may be automatically upgraded, based on the hardware version of the switch. If the boot loader is automatically upgraded, it will take effect on the next reload.

For subsequent Cisco IOS-XE releases, if there is a new bootloader in that release, it may be automatically upgraded based on the hardware version of the switch when you boot up your switch with the new image for the first time.

Caution: Do not power cycle your switch during the upgrade.

Software installation commands

Note: For the **install** command to be successful, it is recommended to have a minimum of free space that is twice the size of the image in flash. If there is not enough space available in flash, you are advised to free up space in flash either by issuing the **install remove inactive** command or to manually clean up the flash by removing unwanted core files or any other files that occupy a large amount of space in flash.

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

Table 9. Summary of software installation commands for install mode

Command	Description
add file tftp: *filename*	Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.
activate [auto-abort-timer]	Activates the file, and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes persistent over reloads.

Command	Description
remove	Deletes all unused and inactive software installation files.

Related resources

Table 10. Additional references for Cisco IE3500 Rugged and IE3500 Heavy Duty Series Switches

Document	Description
Cisco IOS-XE	Provides information about Cisco IOS-XE.
Cisco Warranty Finder	Provides warranty information for a specific product or product family.
Cisco Catalyst IE3500 Rugged Series Switches	Provides information about Cisco Catalyst IE3500 Rugged Series Switches.
Cisco Catalyst IE3500H Heavy Duty Series Switches.	Provides information about Cisco Catalyst IE3500 Heavy Duty Series Switches.
Cisco Validated Designs	Provides Cisco validated designs
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 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.
Documentation Feedback	To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Legal information