Feature removal and suggested alternatives

The following list of features and protocols are planned for eventual removal from Cisco products. The list provides details on why the feature or protocol is considered insecure and suggests secure alternatives when available. Not all platforms and operating systems support all these features.

These features and protocols will be phased out gradually as documented in the deprecation and removal strategy.

Platform-specific details on when each feature will reach the warning, restriction, and removal phases are planned to be provided well in advance of the change.

Feature / Protocol	Why is it insecure?	Recommended Alternative
Plain-text and weak credential storage: Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files	Exposes sensitive data like passwords or pre-shared keys in configuration files.	Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-SHA-256), Type 9 (scrypt), or Type 10 (SHA512) for non-reversible credentials.
SSH Version 1	Many known weaknesses including weak data integrity protection, weak cryptographic algorithms, and other known vulnerabilities	SSH Version 2
SNMPv1 / SNMPv2c	Community strings and data are unencrypted allowing attackers easy access to sensitive data and (in case of SNMP writes) the ability to modify system configuration	SNMPv3 with authentication and encryption (authPriv)
SNMPv3 without authentication and encryption	Without authentication, attackers can send arbitrary SNMP commands to a target	SNMPv3 with authentication and encryption (authPriv)

(noAuthNoPriv or authNoPriv)	device. Without encryption, sensitive data can be exposed on the network.	
MD5 for authentication and 3DES for encryption of SNMPv3 traffic	MD5 is widely considered to be weak and vulnerable to collision vulnerabilities and various attacks. 3DES is weak by modern encryption standards	Use SHA2 (where supported) or SHA1 for authentication. (SHA2 support will be added as part of this initiative to platforms lacking support) Use AES for encryption.
IP source routing based on IP header options	RFC 791 specifies a mechanism for an IP endpoint to specify the path of the packet takes. Attackers can exploit this to facilitate a man-in-the-middle attack.	No exact alternative exists. Customers wanting to control traffic through a network based on source address can do so using policy-based routing or other administrator-controlled source routing mechanisms that do not leave the routing decision to the end user.
TLS 1.0 / TLS 1.1	Formally deprecated by the IETF through RFC 8996 in 2021 due to many cryptographic weaknesses and vulnerabilities including their reliance on SHA1 for message integrity.	Use TLS 1.2 or higher (preferably TLS 1.3) with strong ciphers
TLS ciphers using SHA1 for digital signatures	Susceptible to collision attacks	Use ciphers that use SHA256 or better.
Telnet	Provides no encryption and if authentication is performed, exposes credentials on the network due to the lack of encryption. Can	Use SSH Version 2 for remote management.

	expose keystrokes and other sensitive data.	
FTP	Provides no encryption and if authentication is performed, exposes credentials on the network due to the lack of encryption. Can expose sensitive data such as configuration file contents.	Use SFTP or HTTPS for file transfers
TFTP	Provides no encryption and no authentication or message integrity, making it susceptible to man-in-the-middle and other attacks. Can expose sensitive data such as configuration file contents.	Use SFTP or HTTPS for file transfers. NOTE: TFTP support will be retained in rommon / bootloaders for recovery purposes.
HTTP (with some exceptions like OCSP and SCEP)	Can expose credentials and other sensitive data and is vulnerable to man in the middle attacks because of lack of encryption and message integrity checks.	Use HTTPS. Some features will continue supporting HTTP in limited cases where they do not present a security concern
On-Demand Routing (ODR)	Uses unauthenticated, unencrypted CDP messages to affect network routing tables on network infrastructure.	Use a more modern routing protocol like OSPF, IS-IS, or EIGRP with authentication to protect routing updates from attack.
BootP server	Various security weaknesses allowing rogue devices to affect client boot up behavior.	Use secure bootstrapping features like secure ZTP in conjunction with DHCP. DHCP can be better protected with features like DHCP snooping.

TCP and UDP small servers (echo, chargen, discard, daytime)	Can be used by attackers for denial-of-service attacks and present an elevated attack surface	Discontinue the use of these features. If absolutely needed, these services can be run on a standard Linux host.
IP Finger	Discloses sensitive information without any authentication	Obtain the information provided by the IP Finger service through authenticated management protocols (e.g. SSH sessions)
NTP control messages	Allows an attacker to manipulate the system time on a system, enabling attacks such as a denial of service or allowing for the obfuscation of malicious activities by causing activities to be logged with an incorrect timestamp.	Use 'show' and configuration commands from the device to query or update NTP configuration directly on the device.
TACACS+ using pre-shared keys and MD5	MD5 is generally considered cryptographically weak and compromise of a pre-shared key (especially when the same key is used for many devices) can lead to attackers being able to decode sensitive credentials sent on the network.	Use TACACS+ over TLS 1.3.

As each platform and operating system plans for these changes, we will provide details as to the exact releases and timeframes where you can expect these changes.