Cisco Password Types: Best Practices

Three years ago, the Department of Homeland Security (DHS) released an alert on how cyber adversaries obtained hashed password values and other sensitive information from network infrastructure configuration files. Once the hashes were obtained, the adversaries were able to compromise network devices. That alert showed the results of what happens when cyber adversaries compromise device configurations that have insecure, reversible hashes: they are able to extract sensitive information and compromise networks [1].

NSA recommends using:

- **Multi-factor authentication when feasible**
- **Type 8 for passwords**
- **Type 6 for VPN keys**
- **Strong, unique passwords**
- **Privilege levels for least privilege**

The rise in the number of compromises of network infrastructures in recent years is a reminder that authentication to network devices is an important consideration. Network devices could be compromised due to:

- Poor password choice (vulnerable to brute force password spraying),
- Router configuration files (which contain hashed passwords) sent via unencrypted email, or
- Reused passwords (where passwords recovered from a compromised device can then be used to compromise other devices).

Using passwords by themselves increases the risk of device exploitation. While **NSA strongly recommends multi-factor authentication for administrators managing critical devices**, sometimes passwords alone must be used. Choosing good password storage algorithms can make exploitation much more difficult.

Cisco® devices offer a variety of different password hashing and encryption schemes to secure passwords stored in configuration files. Cisco systems come in a variety of platforms and are widely used within many infrastructure networks worldwide. Cisco networking devices are configured to propagate network traffic among various subnets. They also protect network information that flows into these subnets. The devices contain a plaintext configuration file that is loaded after the Cisco operating system boots. The configuration file:

- Contains specific settings that control the behavior of the Cisco device,
- Determines how to direct traffic within a network, and
- Stores pre-shared keys and user authentication information.

To protect this sensitive data, Cisco devices can use hashing or encryption algorithms to secure this information, but only if they are properly configured to do so.

Hashing is a one-way algorithm. It produces output that is difficult to reverse back to the original string. A random salt is often added to a password prior to hashing, making it difficult to use precomputed hashes to reverse the password. If the salted hash of a strong password (i.e., one that is both long and complex, making it hard for a computer to guess) is captured by a malicious actor, that hash should be of little use since the actor could not recover the actual password.

Encryption is an algorithm that uses a key to produce output that is difficult to reverse back to the original plaintext string without a key. The encryption is either symmetric, which uses the same key for encryption and decryption, or asymmetric, which uses a public key for encryption and a corresponding private key for decryption back to the original string. Cisco Type 6 passwords, for example, allow for secure, encrypted storage of plaintext passwords on the device.

When configuration files are not properly protected, Cisco devices that are configured to use a weak password protection algorithm do not adequately secure the credentials. This can lead to compromised devices, and potentially to compromised entire networks.

Severity of the vulnerability

Hashed or encrypted forms of passwords can be stored in configuration files for authentication purposes to protect the plaintext password. When the configuration file displays on the Command Line Interface, or if it is copied from the device, the user sees the protected form of the password with a number next to it. The number indicates the type of algorithm used to secure the password. The password protection types for Cisco devices are 0, 4, 5, 6, 7, 8, and 9.

For an overview of the Cisco password types, the following table lists them, their difficulty to crack and recover the plaintext password, their vulnerability severity, and

NSA's recommendations for use. For details on each password type, refer to the following sections:

Table: Cisco password types

Password type	Ability to crack	Vulnerability severity	NSA recommendation
Type 0	Immediate	Critical	**Do not use**
Type 4	Easy	Critical	**Do not use**
Type 5	Medium	Medium	**Not NIST approved, use only when Types 6, 8, and 9 are not available**
Type 6	Difficult	Low	**Use only when reversible encryption is needed, or when Type 8 is not available**
Type 7	Immediate	Critical	**Do not use**
Type 8	Difficult	Low	**Recommended**
Type 9	Difficult	Low	**Not NIST approved**

Password types

Type 0

DO NOT USE: Passwords are **NOT** encrypted or hashed. They are stored in plaintext within the configuration file. **NSA strongly recommends against using Type 0**.

Example of a Type 0 password shown in a Cisco configuration:

```
username bob password 0 P@ssw0rd
```

Type 4

DO NOT USE: Introduced around 2013, it uses the Password-Based Key Derivation Function version 2 (PBKDF2) and was originally added to reduce the vulnerability to brute force attempts. However, due to an implementation issue, the Type 4 algorithm only performs a single iteration of SHA-256 (without a salt) over the provided plaintext password, making it weaker than Type 5 and less resistant to brute force attempts. The passwords are stored as hashes within the configuration file. Type 4 was deprecated starting with Cisco operating systems developed after 2013. **NSA strongly recommends against using Type 4.**

Example of a Type 4 password shown in a Cisco configuration:

```
username bob secret 4 g1rTD89b38NIXbGJse.zLc7Cega1TBTlKQNvYDh9Qo6
```

Type 5

NOT NIST APPROVED: Introduced around 1992. It uses a very simple Message-Digest 5 (MD5) hashing algorithm - 1,000 iterations of MD5 with a 32-bit salt. The MD5 algorithm is not NIST approved. Type 5 passwords are relatively easy to brute force with modern computers and tools available on the Internet that make it possible to find collisions for MD5 hashes. The passwords are stored as hashes within the configuration file.

Only use Type 5 if the hardware cannot utilize software that supports Types 6, 8, or 9. NSA also recommends upgrading the hardware to support the newer password encryption algorithms and more recent Internetwork Operating System (IOS®) versions to take advantage of newer security features.

Example of a Type 5 password shown in a Cisco configuration:

```
username bob secret 5 $1$w1Jm$bCt7eJNv.CjWPwyfWcobP0
```

Type 6

USE ONLY WHEN REVERSIBLE ENCRYPTION IS NEEDED OR WHEN TYPE 8 IS NOT AVAILABLE: Type 6 uses a reversible 128-bit Advanced Encryption Standard (AES) encryption algorithm, meaning that the device can decrypt the protected password into the plaintext password. Type 6 is more secure than Type 7 for cases where the device needs the plaintext password, such as for use as virtual private network (VPN) keys. To use Type 6 or convert existing password types (Type 0 or Type 7) to Type 6, configure the primary key with the "`key config-key password-encrypt`" command. This key is not saved in the running configuration file and is used to encrypt and decrypt the passwords.

Then enable AES encryption by issuing the "`password encryption aes`" command. Existing and newly created plaintext passwords are then stored in Type 6 format in the configuration file. **NSA recommends always using Type 6 for VPN keys. Other than for VPN keys, NSA only recommends using Type 6 for passwords if Type 8 is not available (which typically implies that Type 9 is also unavailable).**

Example of a Type 6 password and VPN pre-shared key shown in a Cisco configuration after converting from Type 0 or 7:

```
username bob password 6 fZbe^WdXO`^O[YF`XLCfBV\BK`hMge]HF

crypto isakmp key 6 FLgBaJHXdYY_AcHZZMgQ_RhTDJXHUBAAB
address <ip address>
```

Type 7

DO NOT USE: Uses a simple alphabetical substitution Vigenere cipher with a hardcoded publicly known key. It can be reversed immediately into plaintext by using tools on the Internet. The passwords are stored as encoded strings within the configuration file. Consider them obfuscated, instead of encrypted [2]. **NSA strongly recommends against using Type 7**.

Example of a Type 7 password shown in a Cisco configuration:

```
username bob password 7 08116C5D1A0E550516
```

Type 8

RECOMMENDED: Starting with Cisco operating systems developed after 2013, Type 8 is what Type 4 was meant to be. Type 8 passwords are hashed with the Password-Based Key Derivation Function version 2 (PBKDF2), SHA-256, an 80-bit salt, and 20,000 iterations, which makes it more secure in comparison to the previous password types. The passwords are stored as hashes within the configuration file. Type 8 is less resource intensive than Type 9 passwords. No known issues have been found regarding Type 8 passwords. **NSA recommends using Type 8**.

- To enable Type 8 privilege EXEC mode passwords:

```
Router(config)#enable algorithm-type sha256 secret
<password>
```

- To create a local user account with a Type 8 password:

```
Router(config)#username bob algorithm-type sha256 secret
<password>
```

- Example of a Type 8 password shown in a Cisco configuration:

```
username bob secret 8
$8$kMehFGHe4ew.chRm.d3hge68ECor21viE35NAMV72qPho75fl/lsFlyEFl
```

Type 9

NOT NIST APPROVED: Also starting with Cisco operating systems developed after 2013, Type 9 was introduced using the Scrypt hashing algorithm, with an 80-bit salt, and 16384 iterations. Type 9 is designed to make it difficult to crack the password since it requires a significant amount of hardware resources to do so, raising the cost for an adversary to brute force. The passwords are stored as hashes within the configuration file. Cisco and industry recommend Type 9 hashes. However, the algorithm has not been evaluated against NIST-approved standards and therefore is not recommended by NSA nor approved for use on National Security Systems (NSS).

- To enable Type 9 privilege EXEC mode passwords:

```
Router(config)#enable algorithm-type scrypt secret
<password>
```

- To create a local user account with a Type 9 password:

```
Router(config)#username bob algorithm-type scrypt secret
<password>
```

- Example of a Type 9 password shown in a Cisco configuration:

```
username bob secret 9
$9$ApsgnGtdkTswkfjucj./4w7dcjhGFsjkdT7mAup2lveHuu25fL.hgvfiq
```

Mitigate password storage vulnerabilities

For enterprises utilizing Cisco devices, NSA highly recommends using strong, approved cryptographic algorithms that will protect the password within the configuration file. Password exposure due to a weak algorithm may allow for elevated privileges, which in turn, can lead to a compromised network. Cisco's Type 8 and Type 9 hashing algorithms are available on Cisco operating systems developed after 2013. Network administrators should fully use these methods to protect sensitive credentials. If a network device does not support Type 8 and Type 9 password protection, then the device should be upgraded.

Use Type 8 and refrain from using Type 0, 4, 5, and 7

Type 8 should be enabled and used for all Cisco devices running software developed after 2013. Devices running software from before 2013 should be upgraded

immediately. Types 0, 4, 5, and 7 should not be used on Cisco devices due to weak hashing algorithms that can result in exposing user credentials. Type 6 passwords should only be used if specific keys need to be encrypted and not hashed, or when Type 8 is not available (which typically implies that Type 9 is also unavailable).

Use a strong password for access into privilege EXEC mode

To provide as much protection as possible, use strong passwords to prevent them from being cracked and converted to plaintext. Comply with a password policy that:

- Consists of a combination of lowercase and uppercase letters, symbols, and numbers;
- Is at least 15 alphanumeric characters; and
- Patterns that are not:
  - A keyboard walk
  - The same as a user name
  - The default password
  - The same as a password used anywhere else
  - Related to the network, organization, location, or other function identifiers
  - Straight from a dictionary, common acronyms, or easy to guess

To enforce password complexity, the password policy should be edited to implement complex passwords for each user:

```
Router(config)#aaa new-model
Router(config)#aaa common-criteria policy policy_name
Router(config-cc-policy)#char changes number
Router(config-cc-policy)#max-length number
Router(config-cc-policy)#min-length number
Router(config-cc-policy)#numeric-count number
Router(config-cc-policy)#special-case number
Router(config-cc-policy)#exit
Router(config)#username user common-criteria-policy
policy_name password password
Router(config)#exit
```

Use privilege levels to restrict access

In larger enterprise networks, the level of privileges within the command line should be used to provide role separation. Cisco devices have 16 privilege levels that range from 0 to 15. Level 0 access allows only five commands, while level 15 access allows complete administrative control of the Cisco device. Administrators should customize privilege levels to restrict executing specific commands. Restricting access to specific commands through privilege EXEC mode can prevent certain users from accessing the running configuration. Once the privilege level is customized, an encrypted password can be set for that privilege level. To create a new privilege level for a command, do the following:

```
Router(config)#privilege_mode level [0-15] command_string
Router(config)#enable secret level [0-15] password_string
Router(config)#exit
```

Cisco password types best practices summary

The importance of implementing password security for Cisco network devices will greatly decrease the chances of any network being compromised. If one is mindful of the hash and encryption algorithms that are available within Cisco devices, more secure configurations can be set to prevent password exposure as follows:

- **Use password Type 8.** Do not use Types 0, 4, and 7. Only use Type 5 when Types 6, 8, and 9 are not available, and upgrade hardware and software to support modern hash algorithms. Use password Type 6 when reversible encryption must be used.
- **Use strong password policies to get into privilege EXEC mode.** Along with using strong password hash and encryption algorithms, creating a password that is very difficult to guess can prevent a network compromise. A complex password can prevent an unauthorized user from gaining elevated privileges and exposing the configuration file.
- **Use privilege levels.** Do not apply level 15 to all user accounts. Provision various privileged levels to user accounts and commands based on user roles.

Works cited

[1] Cybersecurity and Infrastructure Security Agency (2018), Alert (TA18-106A) Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices. Available at: https://www.cisa.gov/uscert/ncas/alerts/TA18-106A

[2] S. Singh, Cisco Systems, Inc. (2020), Cisco Guide to Harden Cisco IOS Devices. Available at: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

Related works

- Y. Auda (2020), Cisco Routers Password Types. Available at: https://learningnetwork.cisco.com/s/article/cisco-routers-password-types.
- T. Glen (2021), Understanding the differences between the Cisco password \ secret Types. Available at: https://community.cisco.com/t5/networking-documents/understanding-the-differences-between-the-cisco-password-secret/ta-p/3163238.
- Router-switch.com (2020). Six Types of Cisco Password. Available at: https://www.router.-switch.com/faq/six-types-of-cisco-password.html
- P. Paluch (2013). When to Use Type-6 Encrypted or Type-7 Encrypted? Available at: https://community.cisco.com/t5/switching/when-to-use-type-6-encrypted-or-type-7-encrypted/td-p/2200854.

Trademarks

Disclaimer of endorsement

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov