Password Encryption Improvement

Revision History

Revision Details	Release
First introduced.	21.27.4

Feature Description

The configuration files in CUPS contain many commands for various levels of sensitive information ranging from non-sensitive to highly confidential information. Sensitive information must be protected from unauthorized access from admins or users. There are numerous methods for securing sensitive data which are listed below:

- Symmetrical Encryption.
- Asymmetrical Encryption.
- One-way Hashing.

How it Works

Symmetrical encryption is used to secure sensitive information present in the configuration files, such as remote TACACS+ passwords for client authentication, LI configuration, passwords, SSH key, SNMP community strings, and so on. Sometimes, sensitive information in plain text format is forwarded to the remote servers in CUPS. One example is when the CUPS system acts as the TACACS+ client where a password authentication is required to access the remote TACACS+ server. Once the sensitive information is saved after the one-way hashing process, the system cannot decode or reverse the hash value to obtain the plain text.

CUPS uses symmetrical encryption to address this issue, by allowing the password to be hashed with random salt.

The plain text password is hashed by the system using the **PBKDF2** hash algorithm as follows:

- System generates 16 bytes of random salt from the /dev/urandom device file.
- The number of iterations in **PBKDF2** is calculated as follows:
    - 10000 rounds as base value.
    - Additional rounds based on random salt.
    - The result (hash value) of length 64 bytes.

The hashed password is saved during system configuration process. The plain text password that is entered by the user is then converted to a hash value based on the same salt for comparison the authentication phase.

Note The password hash value is encrypted in such a way as to minimize and avoid any further changes in the existing CLI.

Symmetrical Encryption Occurrences

For various types of data, there are many symmetrical encryption occurrences in CUPS.

Encryption of Smaller and Generic Sensitive Data (fewer than 512 bytes)

CUPS handles the encryption of smaller and generic sensitive data which is lesser than 512 bytes in length.

P2P Library License Expiry to a Persistent File on Flash

The feature P2P license control the P2P libraries with expiry date. P2P licenses have an expiry time which controls the loading of valid P2P libraries. License expiry time from the P2P license is stored in a file for future reference.

Encryption of Long Data (larger than 512 bytes)

Larger size binary text is split into smaller chunks of 512 bytes each. Each of these smaller chunks is then encrypted separately and concatenated together as strings.

SSH Key of CUPS as Client (mgmt interface)

CUPS also acts as SSH client for some transactions. Once the client SSH key gets generated, it is encrypted during configuration and saved. Subsequent system reboots decrypts and uses this SSH key.

Server SSH Key of CUPS (per context)

CUPS acts as SSH server for incoming login connection requests of administrators. SSH key of SSH server gets generated once and encrypted in the configuration and saved. Subsequent system reboots decrypt it and uses the SSH key.

RSA Private Keys of the System

CUPS provides configuration support for RSA certificates and private key in the configuration mode. These private keys are encrypted using symmetrical encryption in the configuration.

Configuring Encryption Password

Encryption of System Level and Admin Passwords

The encryption of system level and admin passwords is explained below.

Admin Passwords in Saved Configuration

System administrators account passwords appear as "**" values in the **show configuration o/p** command. Whereas the passwords are encrypted using the **save configuration o/p** command.

Tech Support Password

Tech support passwords for support and debugging purposes are available in CUPS. Use the following configuration for configuring the tech support password.

```
configure
  tech-support test-commands [encrypted] password
  end
```

Connected Apps Session Password in QvPC-SI Systems

Use the following configuration for configuring the session password.

```
sess-passwd encrypted password
```

ACS Billing

Use the following configuration for configuring the RADIUS user password.

```
cca radius user-password encrypted password password
```

IMS CSCF NPBD Bind IP System Id

Use the following configuration for configuring the IMS CSCF NPBD Bind IP System ID.

```
IMS CSCF NPBD Bind IP System-id sys_id id id encrypted password password
```

SNMP Community String

Use the following configuration for configuring the SNMP Community String.

```
snmp community encrypted password
```

TACACS+ Client Password

Use the following configuration for configuring the TACACS+ Client Password.

```
server priority ip-address ip_address password password
```

BFD Multi-hop Peer Authentication

Use the following configuration for configuring the BFD multihop peer authentication.

bfd multihop-peer *peer_name* **authentication** *authentication* **encrypted password** *password*