Technical Advisory – SSH Lockout

Summary

Customers are experiencing failure to remote login using SSH.

Login is successful when using the console serial connection but fails when using SSH.

Problem Description

Starting with EFOS release 3.4.4.4 many new features were added to enhance the security of the BES switch. They include but are not limited to:

- Password lockout feature is enabled by default. The "passwords lock-out" command currently has a default of 0 (no lockout) - this is changed to 3.

- Enable password complexity

  Default Password complexity has the follow requirement:

  - Minimum Uppercase letters 2
  - Minimum Lowercase letters 2
  - Minimum Numeric characters 2
  - Minimum special characters 2
  - Maximum consecutive characters 0
  - Maximum repeated characters 0
  - Minimum character classes 4

- Force a password change on first login to the switch - SB-327 Information privacy: connected devices

For new switches, on first login, the user must change the default password and it must meet the requirements of the default password complexity requirements. This will result in a password that is more secure but may cause additional attempts to login if the user does not enter the stronger password correctly.

In addition to a more secure password, password lockout will result in a failure to login through SSH if the password is incorrectly entered more than three times. There is no timeout and the lockout remains in effect until the password lockout is set to 0.

27 July 2020

Recovery

1. Physical access to the switch is required and a connection established to the serial console port.
2. Ensure that the customer can login through the serial console.

- If the customer cannot login through the serial console or is not sure of the **admin** password, use the password recovery, option 13, from the boot menu to login without a password prompt:

```
EFOS Startup Rev: 3.4.4

        Select startup mode.  If no selection is made within 3 seconds,
        the EFOS Application will start automatically...

        EFOS Startup -- Main Menu

        1 - Start EFOS Application
        2 - Display Utility Menu

Select (1, 2): 2
    EFOS Startup Rev: 3.4.4

    EFOS Startup -- Utility Menu

    1  - Start EFOS Application
    2  - Load Code Update Package
    3  - Load Configuration
    4  - Select Serial Speed
    5  - Retrieve Error Log
    6  - Erase Current Configuration
    7  - Erase Permanent Storage
    8  - Select Boot Method
    9  - Activate Backup Image
    10 - Start Diagnostic Application
    11 - Reboot
    12 - Erase All Configuration Files
    13 - Start Password Recovery
```

- Change the admin password to a new password:

```
(BES-switch) #configure

(BES-switch) (Config)#username admin password new-password level 15
```

Note: After the password change the running-config must be saved to the startup-config to make the password change persistent

3. Disable password lockout function

```
(BES-switch) #configure

(BES-switch) (Config)# passwords lock-out 0
```

The lockout value must be set to `0` to disable the password lockout and reset the SSH to a non-locked out state. After setting the value to 0, the lockout can be set again to a value between `1-5` to enable the lockout feature.

Note: Saving the running-config is required to make the new setting persistent across reloads.

27 July 2020