Smart Net Total Care Service Update

You may need to update your CSPC root password

A vulnerability in Common Services Platform Collector (CSPC) software has been detected. It could allow a local attacker to access an affected device by using an account that has a static default password with root level privileges. A successful exploit could allow the attacker to log in to the CSPC using the default account.

We have disabled collector software downloads until a fixed version is available. We expect a CSPC software release with the vulnerability fix during the week of May 27th, 2019.

You must change the local system root password, if you have not already done so, to address the vulnerability. You can do this by logging in with the local admin account and using the *pwdreset root* command. See the example below for details:

```
admin# pwdreset root 60

Password for 'root' reset to - xxxxxxxxxx successfully
Password expires in 60 days
Shell is enabled
passwd: all authentication tokens updated successfully

*** Please memorize the new password ***
Lost passwords cannot be recovered. The only alternative to recover
is to reinstall the server.

admin#
```

If you have additional questions, start a discussion in the Community.

Cisco Customer Experience Product Management