New issue

Jump to bottom

buffer overflow in SerialConsole.cpp #27

Open **firmianay** opened this issue on Jul 2 · 1 comment

firmianay commented on Jul 2

hi, great project!

There is a buffer overflow vulnerability in the handleConfigCmd function of the SerialConsole.cpp file. When cmdString == String("FILEEXT")), the newString is copied to fileNameExt without checking the length, and overflow may occur.

```
void SerialConsole::handleConfigCmd()
{
    int i;
    int newValue;
    char *newString;
    bool writeEEPROM = false;
    bool writeDigEE = false;
    char *dataTok;

    if (ptrBuffer < 6)
        return; //4 digit command, =, value is at least 6 characters
    cmdBuffer[ptrBuffer] = 0; //make sure to null terminate
    String cmdString = String();
    unsigned char whichEntry = '0';
    i = 0;

    while (cmdBuffer[i] != '=' && i < ptrBuffer) {
        cmdString.concat(String(cmdBuffer[i++]));
    }
    i++; //skip the =
    if (i >= ptrBuffer) {
        Logger::console("Command needs a value..ie TORQ=3000");
        Logger::console("");
        return; //or, we could use this to display the parameter instead of setting
    }

    newValue = strtol((char *) (cmdBuffer + i), NULL, 0); //try to turn the string into a number
    newString = (char *)(cmdBuffer + i); //leave it as a string

    if (cmdString == String("CAN0EN")) {
```

```
......

    } else if (cmdString == String("FILEBASE")) {
        Logger::console("Setting File Base Name to %s", newString);
        strcpy((char *)settings.fileNameBase, newString);
        writeEEPROM = true;
    } else if (cmdString == String("FILEEXT")) {
        Logger::console("Setting File Extension to %s", newString);
        strcpy((char *)settings.fileNameExt, newString);
        writeEEPROM = true;
```

firmianay commented on Aug 3 • edited ▾ Author

https://nvd.nist.gov/vuln/detail/CVE-2022-35161
Discoverer: Chao Yang@Li Auto

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant