Shruti kapoor Follow
Aug 19 · 2 min read · Listen

Save

CVE-2022–35203

An access control issue in TrenDnet

Discovered by->Shruti Kapoor

model number->TV-IP572PI

version-> 1.0

vendor homepage->http://trendnet.com

BUG DESCRIPTION

A vulnerability in the TrenDnet Web Administrative Interface on Version 1.0 Could allow an Unauthenticated Remote User to access a sensitive part of the system with a high privileged account.

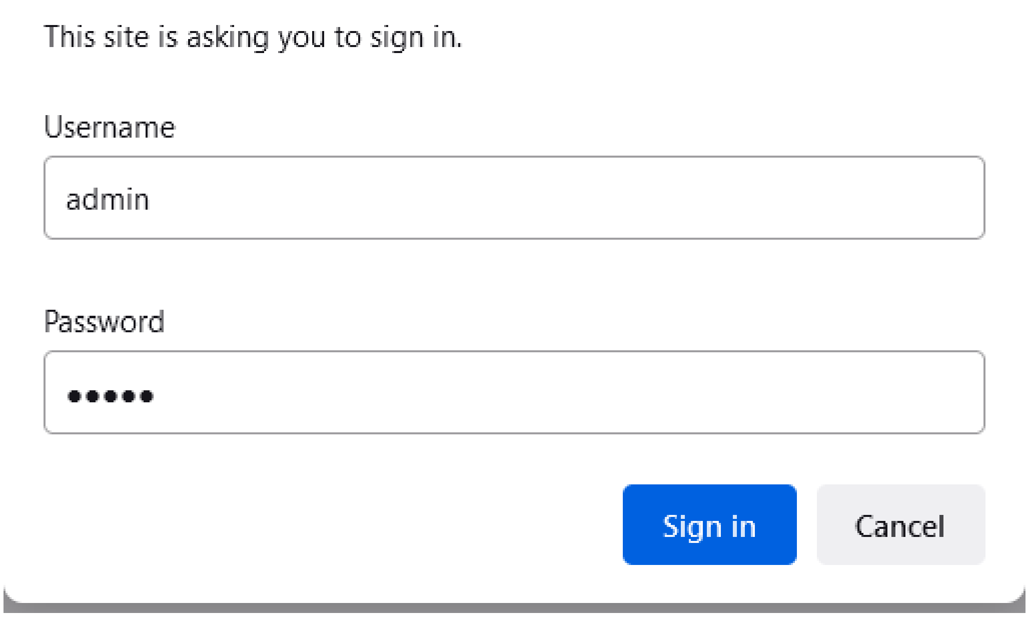
This Vulnerability is Due to the Presence of a Default Account that has a default username “**admin**” and default password “**admin**” in it. An attacker could exploit this vulnerability by using this default account to connect to the affected system. A successful exploit could allow the attacker to obtain read and write access to system data, including the configuration of the affected devices. The attacker would gain access to a sensitive portion of the system and have full administrative rights to control the device. Leading to an Increase in the Severity of the Vulnerability.

6 | 3

Attack Vector:

Steps to Reproduce:

1.Go to TrenDnet admin panel



This site is asking you to sign in.

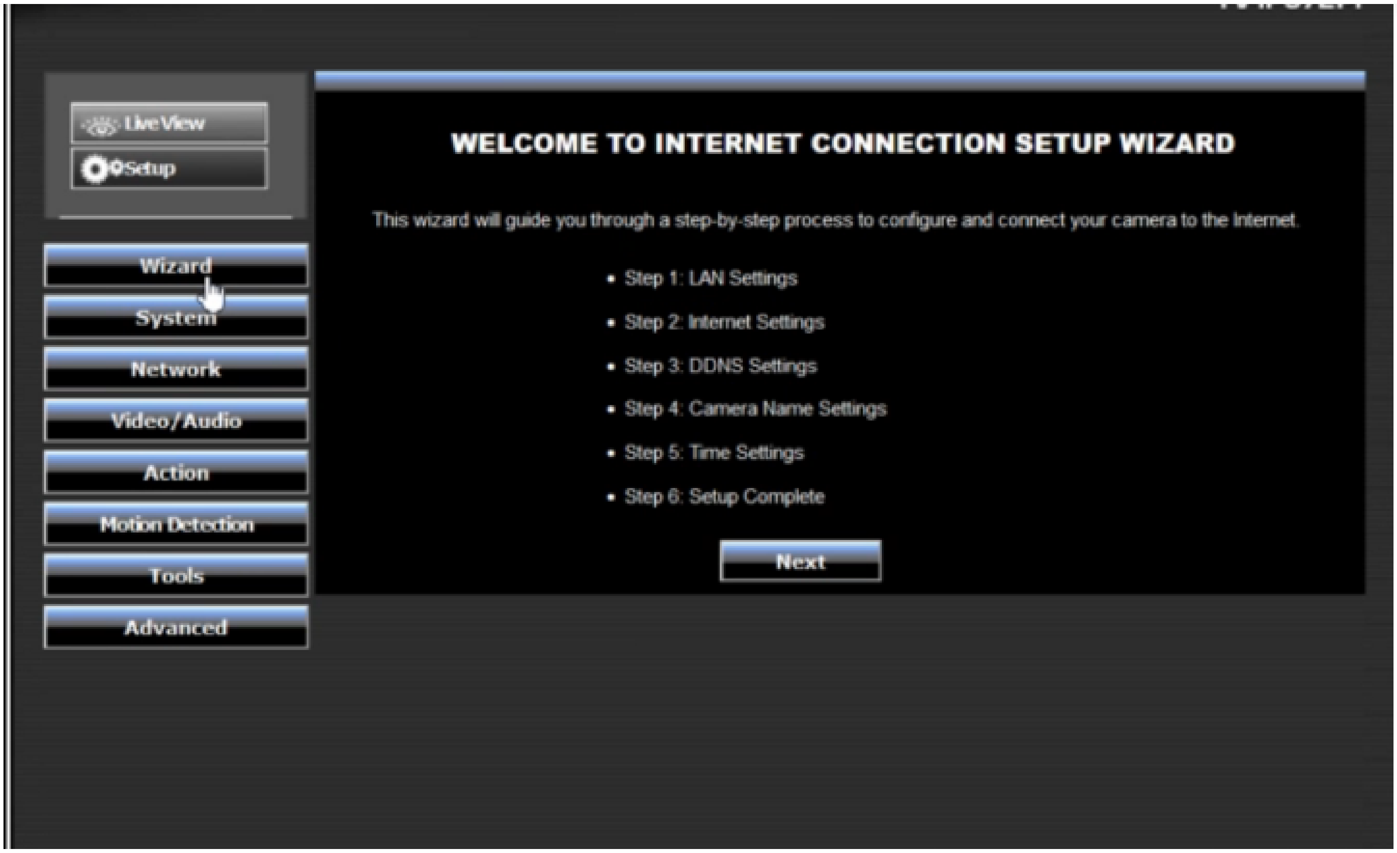
Username: admin

Password: ●●●●●

2. After this you can give the username “admin” and the password “admin” and click on sign in

3.Now when you are Redirected to the Administrative Panel, you will be able to Read and Control the Device and also be able to change the device’s Configuration Remotely.

Proof Of Concept :



WELCOME TO INTERNET CONNECTION SETUP WIZARD

This wizard will guide you through a step-by-step process to configure and connect your camera to the Internet.

- Step 1: LAN Settings
- Step 2: Internet Settings
- Step 3: DDNS Settings
- Step 4: Camera Name Settings
- Step 5: Time Settings
- Step 6: Setup Complete

Thank You for reading :)