

[Open in app](#)[Get started](#)

Dnyanesh Gawande

[Follow](#)

Mar 28 · 2 min read · [Listen](#)



Save



Use of Default Credentials to Unauthorised Remote Access of Internal Panel of Network Video recorder of NUUO

Discovered by Dnyanesh A. Gawande

Published on 24-03-2022.

Vulnerable version ≤ 1.0

Vendor Homepage: <https://nuuo.com/>

CVE ID : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25521>

Bug Description:

A vulnerability in the Nuuo Web Network video recorder Interface on Version 1.0 and Below 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.

Attack Vector:





[Open in app](#)

[Get started](#)

Steps to Reproduce:

1. Go to the NUUO admin panel.



2. After this you can give the username “**admin**” and the password “**admin**” and click on log in.
3. Now when you are Redirected to the Administrative Panel of video recorder, you will be able to Read and Control the Device and also be able to change the device’s Configuration Remotely.

Proof Of Concept :



[Open in app](#)[Get started](#)

NS-8165

- > IP Camera
 - > Camera Settings
 - > Camera Parameters
 - > Camera Status
- > Recording & Event
- > RAID & File System
- > PoE & I/O
- > Network Setup
- > Management
- > System

Camera Settings

Camera Settings | Camera Search

Camera Settings

Camera No. **Camera 1**

Camera Name:

Address: Port:

Administrator Name: Password:

Video Channel: Protocol: ☐ TCP ☐ UDP ☒ HTTP

Brand: Model:

Camera List

No.	Camera Name	Address	Port	Brand	Model
1	cam-101	192.168.1.101	80	Axis	Generic
2	cam-102	192.168.1.102	80	Axis	Generic
3			80	-- none --	-- none --
4			80	-- none --	-- none --
5			80	-- none --	-- none --
6			80	-- none --	-- none --
7			80	-- none --	-- none --
8			80	-- none --	-- none --
9			80	-- none --	-- none --
10			80	-- none --	-- none --
11			80	-- none --	-- none --

Dork to Find

You Can Use the Below Dork to Find the Device Affected. Be Responsible Before Exploiting this Bug.

Shodan : Nuuo

Thank You for reading :)





Open in app

Get started

