Jeya Seelan Follow
Dec 14, 2020 · 2 min read · Listen

CVE-2020-35338

Use of Default Credentials to Unauthorised Remote Access of Internal Panel of WMT

Title: Use of Default Credentials to Unauthorised Remote Access of Internal Panel of WMT

🕵️ Discovered by **Jeya Seelan S**

📝 Published on **14/12/2020.**

💉 **CVE-2020-35338**

📄 **Vulnerable version ≤ 20.2.8**

🔗 **Vendor Homepage:** https://www.mobileviewpoint.com/

CVE Link: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35338

https://vuldb.com/?id.166154

Bug Description:

A vulnerability in the WMT Playout Server's Web Administrative Interface on Version 20.2.8 and Below Could allow an Unauthenticated Remote User to access a sensitive part of the system with a high privileged account.

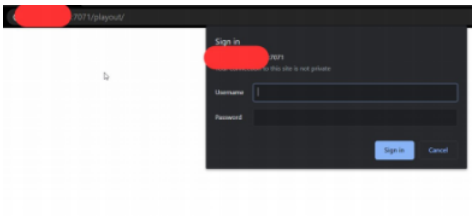
This Vulnerability is Due to the Presence of Default Account that has a default Password "pokon" in it. An attacker could exploit this vulnerability by using this default account to connect to the affected system. A successful exploit could allow the attacker to obtain read and write access to system 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 Increase in the Severity of the Vulnerability.

Attack Vector:

A Malicious attacker could exploit this vulnerability by remotely Logging in to an affected system by using the Default Credentials.

Steps to Reproduce:

1. Go to The Playout Server Login page

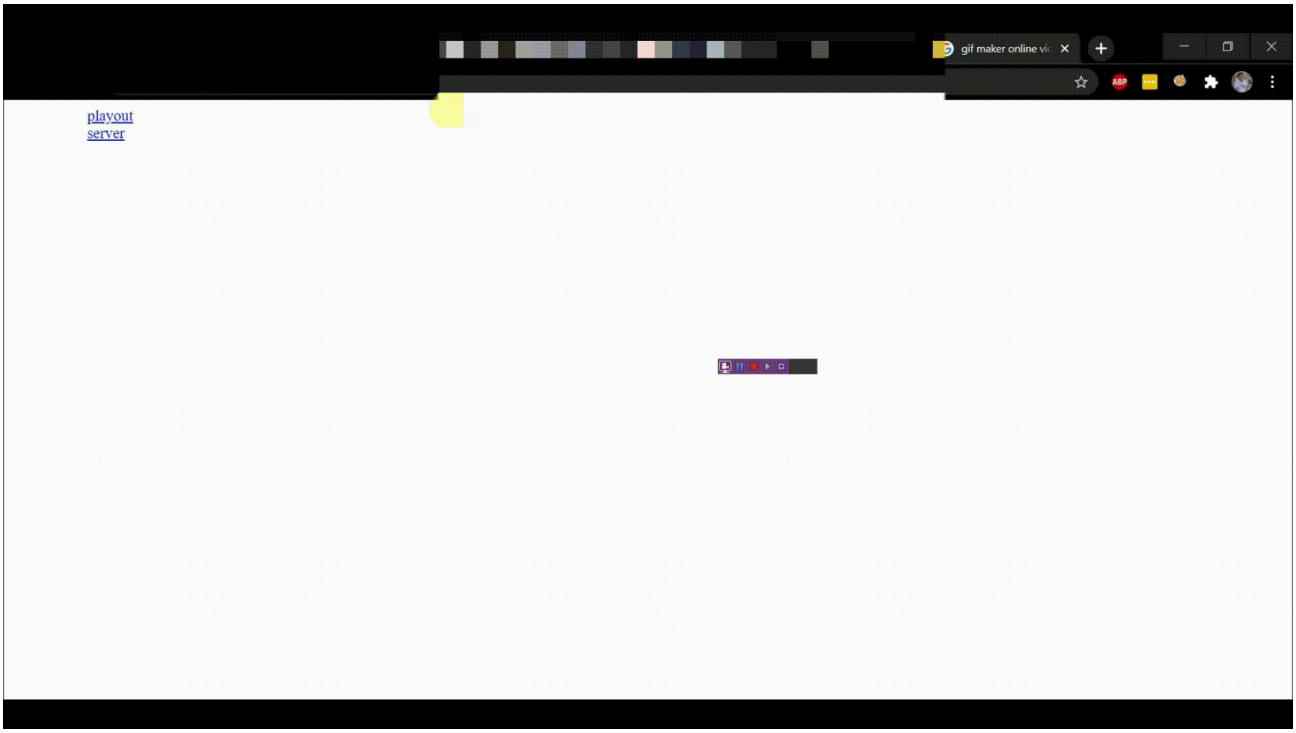


2. Leave the Username Field blank

3. Enter “pokon” on Password Field and Click Sign in

4. Now You are Redirected to the Administrative Panel Where You can Able to Read and Control the Device and also Able to change the device’s Configuration Remotely.

Proof Of Concept:



Dorks to Find

You Can Use the Below Dorks to Find the Devic Affected By this CVE. Be Responsible Before Exploiting this Bug.

Shodan - http.title:WMT

Google — intitle:”WMT” inurl:7071

Cencys : 80.http.get.title: WMT

Thank You for Reading :)