



Yunus Şahin

Follow

Jun 30, 2021 · 1 min read · Listen

Save



RICON Industrial Cellular Router Cleartext Credentials

Model: S9922L

Firmware: 16.10.3(3794)

Hardware: Version: 1.0

CVE: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36165>

RICON Industrial Cellular Router sends username and password as base64.

Request

Pretty Raw Hex In

```
1 GET /asp/setupex/Routing.asp HTTP/1.1
2 Host:
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https:// /asp/fm_menu.htm
8 Upgrade-Insecure-Requests: 1
9 Authorization: Basic YWRtaW46YWRtaW4=
10 Te: trailers
11 Connection: close
12
13
```

YWRtaW46YWRtaW4=

admin:admin

