

- [Home](#)
- [Vulnerabilities](#)
- [Blog](#)
- [Services](#)
- [About](#)
- [Contact](#)



## SOYAL 701Server 9.0.1 Insecure Permissions

Title: SOYAL 701Server 9.0.1 Insecure Permissions

Advisory ID: [ZSL-2021-5633](#)

Type: Local

Impact: Privilege Escalation

Risk: (3/5)

Release Date: 18.03.2021

### Summary

701 Server is the program used to set up and configure LAN and IP based access control systems, from the COM port used to the quantity and type of controllers connected. It is also used for programming some of the more complex controllers such as the AR-716E and the AR-829E.

### Description

The application suffers from an elevation of privileges vulnerability which can be used by a simple authenticated user that can change the executable file with a binary of choice. The vulnerability exist due to the improper permissions, with the 'F' flag (Full) for 'Everyone' and 'Authenticated Users' group.

### Vendor

SOYAL Technology Co., Ltd - <https://www.soyal.com>

### Affected Version

9.0.1 190322

8.0.6 181227

### Tested On

Microsoft Windows 10 Enterprise

### Vendor Status

[25.01.2021] Vulnerability discovered.

[03.02.2021] Vendor contacted.

[08.02.2021] No response from the vendor.

[09.02.2021] Distributor responds and informs vendor.

[09.02.2021] Sent details to distributor.

[10.02.2021] Asked distributor for status update.

[11.02.2021] Vendor will patch the issue.

[18.03.2021] Public security advisory released.

### PoC

[soyal\\_701serverperms.txt](#)

### Credits

Vulnerability discovered by Gjoko Krstic - [<gjoko@zeroscience.mk>](mailto:gjoko@zeroscience.mk)

### References

[1] <https://packetstormsecurity.com/files/161877/>

[2] <https://www.exploit-db.com/exploits/49678>

[3] <https://cxsecurity.com/issue/WLB-2021030142>

[4] <https://exchange.xforce.ibmcloud.com/vulnerabilities/198550>

[5] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28271>

[6] <https://nvd.nist.gov/vuln/detail/CVE-2021-28271>

### Changelog

[18.03.2021] - Initial release

[23.03.2021] - Added reference [1], [2], [3] and [4]

[19.06.2021] - Added reference [5] and [6]

### Contact

Zero Science Lab

Web: <https://www.zeroscience.mk>

e-mail: [lab@zeroscience.mk](mailto:lab@zeroscience.mk)

## • Rete mirabilia

## • We Suggest

- **Profiles**



-  [Site Meter](#)