- Home
- Vulnerabilities!
- Blog
- Services
- About
- Contact

SOYAL 701Client 9.0.1 Insecure Permissions

Title: SOYAL 701Client 9.0.1 Insecure Permissions
Advisory ID: ZSL-2021-5634
Type: Local
Impact: Privilege Escalation
Risk: (3/5)
Release Date: 18.03.2021

Summary

701 Client is the user interface software for the access control system. It is used for adding and deleting tokens, setting door groups for access, setting time zones for limiting access and monitoring ingress and egress on a live system, among other things.

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 'Authenticated Users' group.

Vendor

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

Affected Version

9.0.1 190410
9.0.1 190115

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_701clientperms.txt

Credits

Vulnerability discovered by Gjoko Krstic - <gjoko@zeroscience.mk>

References

[1] https://www.exploit-db.com/exploits/49679
[2] https://packetstormsecurity.com/files/161878/
[3] https://cxsecurity.com/issue/WLB-2021030135
[4] https://exchange.xforce.ibmcloud.com/vulnerabilities/198548
[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28269
[6] https://nvd.nist.gov/vuln/detail/CVE-2021-28269
[7] https://www.tenable.com/cve/CVE-2021-28269
[8] https://www.security-database.com/detail.php?alert=CVE-2021-28269

Changelog

[18.03.2021] - Initial release
[23.03.2021] - Added reference [1], [2], [3] and [4]
[19.06.2021] - Added reference [5], [6], [7] and [8]

Contact

Zero Science Lab

Web: https://www.zeroscience.mk
e-mail: lab@zeroscience.mk

- # Rete mirabilia

- # We Suggest

- **Profiles**

- Site Meter