

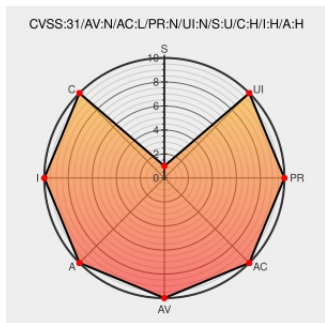


# CVE-2020-3934

Published on: 02/11/2020 12:00:00 AM UTC

Last Modified on: 01/01/2022 07:58:00 PM UTC

## CVE-2020-3934

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Dr.id Access Control](#) from [Secom](#) contain the following vulnerability:

TAIWAN SECOM CO., LTD., a Door Access Control and Personnel Attendance Management system, contains a vulnerability of Pre-auth SQL Injection, allowing attackers to inject a specific SQL command.

CVE-2020-3934 has been assigned by [cve@cert.org.tw](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [TAIWAN SECOM CO., LTD.](#) - **Door Access Control system** version **<= 3.3.2**

Affected Vendor/Software: [TAIWAN SECOM CO., LTD.](#) - **Personnel Attendance system** version **<= 3.3.0.3\_20160517**

CVSS3 Score: **9.8 - CRITICAL**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **7.5 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description | Tags | Link |
|-------------|------|------|
|-------------|------|------|

|                                                                                                                                                                                |                                                                                                                                   |                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CHI Security Red Team Discovered Several Vulnerabilities in Well-Known Domestic Door Access Control and Personnel Attendance Management System   中華資安國際 CHT Security Co., Ltd. | <a href="#">Third Party Advisory</a><br><a href="http://www.chtsecurity.com">www.chtsecurity.com</a><br><a href="#">text/html</a> |  <a href="https://www.chtsecurity.com/news/1bb851cd-9048-4587-b4d3-b18335572bac">MISC www.chtsecurity.com/news/1bb851cd-9048-4587-b4d3-b18335572bac</a> |
| Dr.ID SQL Injection and Information exposure - GitHub                                                                                                                          | <a href="#">Third Party Advisory</a><br><a href="https://gist.github.com">gist.github.com</a><br><a href="#">text/html</a>        |  <a href="https://gist.github.com/chtsecurity/4db471b34c3959e5ab9ec31570e4760b">MISC gist.github.com/chtsecurity/4db471b34c3959e5ab9ec31570e4760b</a> |
| TWCERT/CC Taiwan Computer Emergency Response Team/Coordination Center-TAIWAN SECOM CO., LTD. - Pre-auth SQL Injection                                                          | <a href="http://www.twcert.org.tw">www.twcert.org.tw</a><br><a href="#">text/html</a>                                             |  <a href="https://www.twcert.org.tw/en/cp-139-3318-89f76-2.html">MISC www.twcert.org.tw/en/cp-139-3318-89f76-2.html</a>                               |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type                                                            | Vendor                | Product                                 | Version          | Update | Edition | Language |
|-----------------------------------------------------------------|-----------------------|-----------------------------------------|------------------|--------|---------|----------|
| Application                                                     | <a href="#">Secom</a> | <a href="#">Dr.id Access Control</a>    | All              | All    | All     | All      |
| Application                                                     | <a href="#">Secom</a> | <a href="#">Dr.id Access Control</a>    | 3.3.2            | All    | All     | All      |
| Application                                                     | <a href="#">Secom</a> | <a href="#">Dr.id Access Control</a>    | 3.3.2            | All    | All     | All      |
| Application                                                     | <a href="#">Secom</a> | <a href="#">Dr.id Attendance System</a> | All              | All    | All     | All      |
| Application                                                     | <a href="#">Secom</a> | <a href="#">Dr.id Attendance System</a> | 3.3.0.3_20160517 | All    | All     | All      |
| Application                                                     | <a href="#">Secom</a> | <a href="#">Dr.id Attendance System</a> | 3.3.0.3_20160517 | All    | All     | All      |
| cpe:2.3:a:secom:dr.id_access_control:*****:                     |                       |                                         |                  |        |         |          |
| cpe:2.3:a:secom:dr.id_access_control:3.3.2:*****:               |                       |                                         |                  |        |         |          |
| cpe:2.3:a:secom:dr.id_access_control:3.3.2:*****:               |                       |                                         |                  |        |         |          |
| cpe:2.3:a:secom:dr.id_attendance_system:*****:                  |                       |                                         |                  |        |         |          |
| cpe:2.3:a:secom:dr.id_attendance_system:3.3.0.3_20160517:*****: |                       |                                         |                  |        |         |          |
| cpe:2.3:a:secom:dr.id_attendance_system:3.3.0.3_20160517:*****: |                       |                                         |                  |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)