



# CVE-2019-19986

Published on: 02/26/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

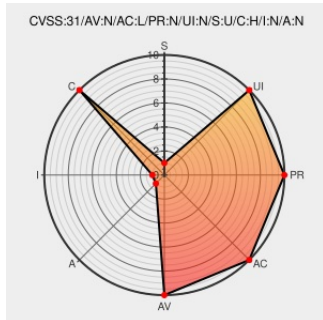
## CVE-2019-19986

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Visual Access Manager](#) from [Seling](#) contain the following vulnerability:

An issue was discovered in Selesta Visual Access Manager (VAM) 4.15.0 through 4.29. An attacker without authentication is able to execute arbitrary SQL SELECT statements by injecting the HTTP (POST or GET) parameter persoid into /tools/VamPersonPhoto.php. The SQL Injection type is Error-based (this means that relies on error messages thrown by the database server to obtain information about the structure of the database).

CVE-2019-19986 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

| 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>NONE</b>         | <b>NONE</b>         |

CVSS2 Score: **5 - MEDIUM**

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

## CVE References

| Description                                      | Tags                    | Link                                |
|--------------------------------------------------|-------------------------|-------------------------------------|
| Controlle access; elevations; execute a Building | <a href="#">Exploit</a> | <a href="#">MISC:www.seling.it/</a> |

|                                                                                  |                                                                                                                                       |                                                                                                                                                                                |
|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Controllo accessi, rilevazione presenze e Building Security - Selesta Ingegneria | <a href="#">Product</a><br><a href="#">www.seling.it</a><br><a href="#">text/html</a>                                                 |  MISC <a href="#">www.seling.it</a>                                                             |
| Applicativo Controllo Accessi: VAM - Selesta Ingegneria                          | <a href="#">Product</a><br><a href="#">Vendor Advisory</a><br><a href="#">www.seling.it</a><br><a href="#">text/html</a>              |  MISC <a href="#">www.seling.it/product/vam/</a>                                              |
| Gruppo TIM   Vulnerability Research & Advisor                                    | <a href="#">Exploit</a><br><a href="#">Third Party Advisory</a><br><a href="#">www.telecomitalia.com</a><br><a href="#">text/html</a> |  MISC<br><a href="#">www.telecomitalia.com/tit/it/innovazione/cybersecurity/red-team.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="#">Seling</a> | <a href="#">Visual Access Manager</a> | All     | All    | All     | All      |
| cpe:2.3:a:seling:visual_access_manager:*****:* |                        |                                       |         |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)