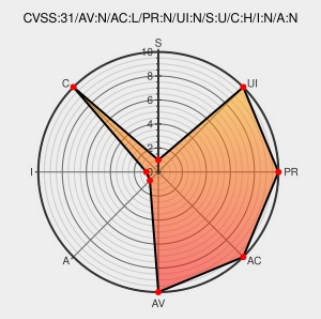
CVE-2019-19986

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 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
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Controllo accessi, rilevazione presenze e Building	Product	MISC www.seling.it/

Controllo accessi, rilevazione presenze e Building Security - Selesta Ingegneria	Product www.seling.it text/html	MISC www.seling.it/
Applicativo Controllo Accessi: VAM - Selesta Ingegneria	Product Vendor Advisory www.seling.it text/html	MISC www.seling.it/product/vam/
Gruppo TIM | Vulnerability Research & Advisor	Exploit Third Party Advisory www.telecomitalia.com text/html	MISC www.telecomitalia.com/tit/it/innovazione/cybersecurity/red-team.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Seling	Visual Access Manager	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→