



## Stored Cross Site Scripting in webserver administration

IDEMIA-SA-2023-08 ACCESS AND TIME BIOMETRIC TERMINALS

September 2023

### >> AFFECTED PRODUCT(S)

SIGMA Lite & Lite +, SIGMA Wide, SIGMA Extreme, MorphoWave Compact/XP, VisionPass, MorphoWave SP

### >> AFFECTED VERSION(S)

Product	Affected versions
SGIMA Lite & Lite+	all
SIGMA Wide	
SIGMA Extreme	
MorphoWave Compact/SP	all
VisionPass	
MorphoWave SP	all

### >> SECURITY RATING: HIGH

>> POTENTIAL IMPACT : Unauthorized access, Data leakage

### >> SUMMARY

**This advisory is only applicable if you are not using the enforced security configuration (\*) because it deactivates the webserver administration panel**

This advisory aims at informing of a Stored Cross-Site Scripting (Stored XSS) vulnerability present in all firmware version of IDEMIA Biometric Terminals for Access and Time. Successful exploitation could lead to data leakage or unauthorized actions performed via the device's administration web interface.





- 2.9 for VisionPass
- 2.9 for MorphoWave Compact / XP
- 1.1 for MorphoWave SP

