Stored Cross Site Scripting in webserver administration IDEMIA-SA-2023-08 ACCESS AND TIME BIOMETRIC TERMINALS

September 2023

AFFECTED PRODUCT(S)

 \gg

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

AFFECTED VERSION(S)

Product	Affected versions
SGIMA Lite & Lite+	
SIGMA Wide	all
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.



CVE-2023-4667: Stored Cross Site Scripting in webserver administration

Severity: HIGH

Base Score: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L - 8.3- HIGH

<u>Description</u>: The web interface of the impacted device allows the administrator user profile to store malicious scripts in certain fields. The stored malicious script is then executed when the GUI is opened by any users of the webserver. Resulting in scripts execution in the targeted user web browser.



The root cause of the vulnerability is inadequate input validation and output encoding in the web administration interface component of the firmware.

Deactivate the webserver. In IDEMIA default and recommended configuration for Access and Time terminals, the administration is done via MorphoManager or other TLS-based software.

We recommend not to use the Webserver functionality in production environment; it is deactivated in the default configuration of the device (*).

IDEMIA will publish a firmware that fixes this issue and update the document accordingly.

WORKAROUND

If you are using the webserver, you should reassess the needs to do so for a production environment. In this case, to mitigate the risk, customers should restrict access to the webserver to trusted users only.

Running the device in a segregated dedicated network is recommended and will also mitigate the risk.

We would like to thank Rayan Almutairi for helping identify this vulnerability.

2023-09-15: initial release

DISCLAIMER

This document is provided "as is" without any express or implied warranty. While every effort has been made to ensure the accuracy of the information contained in this article, the author/maintainer/contributor and/or the company assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein. Information in this advisory can change without notice. Always consult a professional to understand the implications of using or acting upon the information provided in this advisory.

(*) Firmware version:

• 2.12 for SIGMA range terminals

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