Security Advisory

Firmware updates to fix multiple vulnerabilities

IDEMIA-SA-2023-05 ACCESS AND TIME BIOMETRIC TERMINALS

November 2023

AFFECTED PRODUCT(S)

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

AFFECTED VERSION(S)

Product	Affected versions
SIGMA Lite & Lite+	Firmware below 4.15.5 (exclusive)
SIGMA Wide	
SIGMA Extreme	
MorphoWave Compact/XP	Firmware below 2.12.2 (exclusive)
VisionPass	
MorphoWave SP	Firmware below 1.2.7 (exclusive)

SECURITY RATING: CRITICAL

POTENTIAL IMPACT

Unauthorized access, Data leakage or manipulation, and Denial of services

SUMMARY

This security advisory announces fixes for multiple vulnerabilities discovered in Physical Access control devices. They can under certain circumstances lead to arbitrary code execution, or to permanent denial of service.

DETAILED DESCRIPTION

■ CVE-2023-33217: Missing integrity check on upgrade package

Severity

Base score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H - 7.5 -HIGH

Alternative score: if you have kept the default Enforced Security mode or enabled the mTLS to identify the origin of the command issued to the terminal then the severity becomes CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N - 4.9 - MEDIUM

Description

By abusing a design flaw in the firmware upgrade mechanism of the impacted terminal it's possible to cause a permanent denial of service for the terminal. the only way to recover the terminal is by sending back the terminal to the manufacturer.

- **CVE-2023-33218: Stack Buffer Overflow in a binary run at upgrade startup**

Severity

Base score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N - 9.1 - CRITICAL

Alternative score: if you have kept the default Enforced Security mode or enabled the mTLS to identify the origin of the command issued to the terminal then the severity becomes CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N - 6.5 - MEDIUM

Description

The Parameter Zone Read and Parameter Zone Write command handlers allow performing a Stack buffer overflow. This could potentially lead to a Remote Code execution on the targeted device.

- **CVE-2023-33219: Stack Buffer Overflow when checking retrofit package**

Severity

Base score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N - 9.1 - CRITICAL

Alternative score: if you have kept the default Enforced Security mode or enabled the mTLS to identify the origin of the command issued to the terminal then the severity becomes CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N - 6.5 - MEDIUM

Description

The handler of the retrofit validation command doesn't properly check the boundaries when performing certain validation operations. This allows a stack-based buffer overflow that could lead to a potential Remote Code Execution on the targeted device.

- **CVE-2023-33220: Stack Buffer Overflow when checking some attributes during retrofit**

Severity

Base score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N - 9.1 - CRITICAL

Alternative score: if you have kept the default Enforced Security mode or enabled the mTLS to identify the origin of the command issued to the terminal then the severity becomes CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N - 6.5 - MEDIUM

Description

During the retrofit validation process, the firmware doesn't properly check the boundaries while copying some attributes to check. This allows a stack-based buffer overflow that could lead to a potential Remote Code Execution on the targeted device.

- **Heap Buffer Overflow when reading DESFire card - CVE-2023-33221:**

Severity

Base score: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H - 7.8 - HIGH

Description

When reading DesFire keys, the function that reads the card isn't properly checking the boundaries when copying internally the data received. This allows a heap based buffer overflow that could lead to a potential Remote Code Execution on the targeted device. This is especially problematic if you use Default DESFire key.

- **Stack buffer overflow when reading DESFire card - CVE-2023-33222:**

Severity

Base score: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N - 9.1 - CRITICAL

Description

When handling contactless cards, usage of a specific function to get additional information from the card which doesn't check the boundary on the data received while reading. This allows a stack-based buffer overflow that could lead to a potential Remote Code Execution on the targeted device.

CAUSE

The vulnerabilities arise from lack of boundaries check when manipulating buffers, or improper check of firmware update file structure.

RESOLUTION

Update your device firmware to the non-vulnerable version:

Product	Non vulnerable versions
SIGMA Lite & Lite+	Firmware 4.15.5 or higher
SIGMA Wide	
SIGMA Extreme	
MorphoWave Compact/XP	Firmware 2.12.2 or higher
VisionPass	
MorphoWave SP	Firmware 1.2.7 or higher

WORKAROUND

- For all described vulnerabilities except CVE-2023-33222: activate mTLS on the device by following your user manual to prevent arbitrary source from issuing thrift command
- For CVE-2023-33221, CVE-2023-33222: ensure your device uses diversified DESFire keys
- For CVE-2023-33222: there is no workaround, although the attacker needs to have physical access to the device

ACKNOWLEDGEMENT

We would like to thank Lucas Georges from Synacktiv for helping identify those vulnerabilities.

REVISION HISTORY

Date	Content
September 2023	Initial release
November 2023	Typo fix for the other name of MorphoWave Compact (XP and not SP) Update of the version number for MorphoWave SP

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.