BIOMETRIC TERMINALS SECURITY BULLETIN
SB-IDEMIA-2021-01

CORRECTION OF BUFFER OVERFLOW AND PATH TRAVERSAL IN SOME ACCESS CONTROL DEVICES

PHYSICAL ACCESS CONTROL – TIME & ATTENDANCE APPLICATIONS

July 2021

1. SUMMARY

IDEMIA is releasing firmware updates integrating fixes to mitigate security vulnerabilities identified on some IDEMIA physical Access Control devices. Under certain conditions, these vulnerabilities allow code execution, or read and write access to any file from the device.

2. VULNERABILITIES DETAILS

CVEID: CVE-2021-35522

CWE ID: CWE-121: Stack-based Buffer Overflow

An attacker operating from the network can exploit a stack buffer overflow on some thrift command handling functions to perform a remote code execution on a device running the vulnerable firmware. This can potentially impact the integrity and confidentiality of data stored in the device or cause unavailability of the device.

CVSS Base Score: 9.8 (Critical)

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVEID: CVE-2021-35520

CWEID: CWE-122: Heap-based Buffer Overflow

An attacker having physical access and the adequate private key can exploit a heap-based buffer overflow in some thrift command handling functions that can lead to a remote code execution. This can potentially affect integrity, confidentiality, or availability of data stored in the device or cause unavailability of the device

CVSS Base Score: 6.2 (Medium)

CVSS Vector: CVSS3.1/AV:P/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVEID: CVE-2021-35521

CWEID: CWE-23: Relative Path Traversal

An attacker operating from a network and having the adequate private key can exploit a path traversal vulnerability in the thrift command handler to arbitrary, read or write of files in the file system. This can potentially have an impact on the integrity or confidentiality of data stored on the device.

CVSS Base Score: 5.9 (Medium)

CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N

3. AFFECTED PRODUCTS AND PATCHED VERSIONS

Products	CVE-2021-35522	CVE-2021-35520	CVE-2021-35521	Patched version
Morpho*Wave* Compact MD	X		X	2.6.2
Morpho*Wave* Compact MDPI	X	X	X	2.6.2
Morpho*Wave* Compact MDPI-M	X	X	X	2.6.2
VisionPass MD	X		X	2.6.2
VisionPass MDPI	X	X	X	2.6.2
VisionPass MDPI-M	X	X	X	2.6.2
SIGMA Lite (all variants)	X			4.9.4
SIGMA Lite+ (all variants)	X			4.9.4
SIGMA Wide (all variants)	X			4.9.4
SIGMA Extreme	X			4.9.4
MA VP MD	X			4.9.7

Table 1 list of impacted products and patched version

4. REMEDIATION/FIXES

The vulnerabilities can be fixed by using the usual process to update the device to the non-vulnerable software. Refer to the table above to know which version of software to download.

5. WORKAROUNDS AND MITIGATION

Application of TLS server authentication on the device and feeding it with the public certificate of the access control server mitigate the aforementioned vulnerabilities. To see how to activate, refer to your device user manual to apply this configuration.

6. ACKNOWLEDGEMENT

We would like to thank Natalya Tlyapova, Sergey Fedonin, Vladimir Kononovich, and Vyacheslav Moskvin from Positive Technologies for helping us further improve the security of our products.

7. NEED SUPPORT?

If you require support or assistance about implementing the recommendations of this Security Bulletin, please contact the following support services by email or phone.

Region	Email	Phone
North America	support.bioterminals.us@idemia.com	+1 888 940 7477
South America	support.bioterminals.us@idemia.com	+1 714 575 2973
Europe, Middle-East, Africa	support.bioterminals@idemia.com	+33 1 30 20 30 40
Asia, Pacific	support.bioterminals.in@idemia.com	+91 8929159665
India	support.bioterminals.in@idemia.com	+91 1800 120 203 020

For other issues about the content of this Security Bulletin, send e-mail to secure@idemia.com