



TLS PROTOCOL ACTIVATION

PHYSICAL ACCESS CONTROL – TIME & ATTENDANCE APPLICATIONS

December 2021

1. SUMMARY

IDEMIA reminds customers that, in operation and according to section 7 of the document “[Recommendations for a secure installation](#)”, they have to activate and properly configure the TLS protocol. This prevents arbitrary usage of the “trigger_relay” and “terminal_reboot” commands.

IDEMIA also advises customers to make their own security risk assessment with respect of this bulletin and their deployment environment.

2. VULNERABILITIES DETAILS

CVEID: N/A

Internal reference: VU-2021-004

In case TLS protocol is not activated, an attacker operating from the network can use without authentication:

- the “trigger_relay” command to open a door or a turnstile if the terminal directly controls them (Single Door Access Control case)
- or the “terminal_reboot” command to cause denial of service.

CVSS Base Score: 9.1 (Critical)

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 VERSIONS

| Products | Affected version |
|----------------------------|------------------|
| MorphoWave Compact MD | All versions |
| MorphoWave Compact MDPI | All versions |
| MorphoWave Compact MDPI-M | All versions |
| VisionPass MD | All versions |
| VisionPass MDPI | All versions |
| VisionPass MDPI-M | All versions |
| SIGMA Lite (all variants) | All versions |
| SIGMA Lite+ (all variants) | All versions |
| SIGMA Wide (all variants) | All versions |
| SIGMA Extreme | All versions |
| MA VP MD | All versions |

Table 1 list of impacted products and patches

➤ 4. REMEDIATION/FIXES

Activation, proper configuration of TLS protocol and installation of the TLS certificate on the device fixes the aforementioned vulnerability. To see how to activate TLS authentication, please refer to your device user manual.

In a future version of firmware, IDEMIA will make TLS activation mandatory by default.

➤ 5. WORKAROUNDS AND MITIGATION

Refer to section 4.

➤ 6. CREDITS

Natalya Tlyapova, Sergey Fedonin, Vladimir Kononovich, and Vyacheslav Moskvina from Positive Technologies

➤ 7. NEED SUPPORT?

If need 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 an e-mail to secure@idemia.com.