PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

11 August 2021
300521738

Security Advisory for FL MGUARD DM version 1.12.0 and 1.13.0

Advisory Title

Access to the Apache web server being installed as part of the FL MGUARD DM on Microsoft Windows does not require login credentials even if configured during installation.

Advisory ID

CVE-2021-34579
VDE-2021-035

Vulnerability Description

Unauthorized users can download mGuard configuration profiles from the Apache web server without providing credentials (CWE-269 Improper Privilege Management).

Affected products

Article no	Article	Affected versions
2981974	FL MGUARD DM	1.12.0
2981974	FL MGUARD DM	1.13.0

The product is affected if it has been installed with the Microsoft Windows installer, and if it has been configured during installation such that access to the Apache web server is protected by username and password.

Impact

Attackers with network access to the Apache web server can download and therefore read mGuard configuration profiles (“ATV profiles”). Such configuration profiles may contain sensitive information, e.g. private keys associated with IPsec VPN connections.

Classification of Vulnerability

Base Score: 7.5
Vector: CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Temporary Fix / Mitigation

- Stop the ApacheMDM Windows service.
- Edit file `<mdm>/apache/conf/extra/httpd-mdm.conf` and remove the instances of these lines for “DocumentRoot” and alias “/atv”:

  ```
  # Controls who can get stuff from this server.
  Require all granted
  ```

  `<mdm>` refers to the directory in which FL MGUARD DM is installed.
- Start the ApacheMDM Windows service.

Remediation

This vulnerability is fixed in FL MGUARD DM 1.13.0.1. We advise all affected FL MGUARD DM 1.12.0 and 1.13.0 users to upgrade to FL MGUARD DM 1.13.0.1 or a later version.
Additional recommendations:

- Limit network access to the Apache web server to as few network addresses as possible.
- If possible, make use of encrypted mGuard configuration profiles.

Acknowledgement

We kindly appreciate the coordinated disclosure of this vulnerability by the finder.

PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.