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

12 April 2022
300546916

Security Advisory for mGuard Device Manager

Advisory Title

A vulnerability was found in the Apache webserver that allows HTTP Request Smuggling.

Advisory ID

CVE-2022-22720
VDE-2022-014

Vulnerability Description

Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling. For the mGuard Device Manager only the mdm Installer for Windows is affected.

Affected product

Article no	Article	Affected versions	Fixed version
2981974	FL MGUARD DM UNLIMITED	<= 1.13.0.1	Download

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.

Personally liable partner:
Phoenix Contact Verwaltungs GmbH
Amtsgericht Lemgo HRB 5273
Kom. Ges. Amtsgericht Lemgo HRA 3746

Group Executive Board:
Frank Stührenberg (CEO)
Dirk Görlitzer, Torsten Janwlecke
Ulrich Leidecker
Frank Possel-Dölken, Axel Wachholz

Deutsche Bank AG
(BLZ 360 700 50) 226 2665 00
BIC: DEUTDEDEXXX
IBAN:
DE93 3607 0050 0226 2665 00

Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADEFFXXX
IBAN:
DE31 4764 0051 0226 0396 00

...

Classification of Vulnerability

Base Score: 9.8
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Temporary Fix / Mitigation

This vulnerability is exploitable only if the ConfigPull functionality is used and config files are stored unencrypted. As a best practice and mitigation measure, we recommend storing configuration files encrypted with the device specific public key of the mGuard appliances.

Remediation

PHOENIX CONTACT strongly recommends upgrading FL MGUARD DM UNLIMITED to version 1.13.0.2 or higher, which fixes this vulnerability.

Acknowledgement

This vulnerability was discovered by James Kettle.

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.