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

10 November 2021
300524757

Security Advisory for FL MGUARD 1102/1105

Advisory Title

Cross-site scripting in web-based management and memory leak in the remote logging function of FL MGUARD 1102 and FL MGUARD 1105

Advisory ID

CVE-2021-34582
CVE-2021-34598
VDE-2021-046

Vulnerability Description

CVE-2021-34582:
The file upload functionality in the web-based management is affected by a stored cross-site scripting vulnerability (CWE-79: Improper Neutralization of Input During Web Page Generation).

An authenticated FL MGUARD user with *Admin* or *Super Admin* role can upload a certificate file on the **Basic settings > LDAP** page, on the **Logs > Remote logging** page, or through the REST API. The content of this file is embedded into the corresponding web page, and any HTML code within the file is rendered when the page is viewed by the same or a different authenticated user.

CVE-2021-34598:
The remote logging functionality is impaired by the lack of memory release for data structures from syslog-ng when remote logging is active (CWE-770: Allocation of Resources Without Limits or Throttling).

Affected products

Article no	Article	Affected versions
1153079	FL MGUARD 1102	1.4.0, 1.4.1, 1.5.0
1153078	FL MGUARD 1105	1.4.0, 1.4.1, 1.5.0

Impact

CVE-2021-34582:
By embedding a crafted file into the **Logs > Remote logging** page, an authenticated user with *Admin* role can read and/or modify settings only accessible to users with *Super Admin* role (e.g. user settings, LDAP settings). A successful exploit requires that a user with *Super Admin* role views the **Logs > Remote logging** page.
A user with *Admin* role has no access to the settings on the **Basic settings > LDAP** page, and can therefore exploit the vulnerability only on the **Logs > Remote logging** page.

By embedding a crafted file into the **Basic settings > LDAP** or **Logs > Remote logging** page, an authenticated user can modify settings as another user, thereby misrepresenting the identity of the user who made the modifications in the logs. A successful exploit requires the other user to view the **Basic settings > LDAP** or **Logs > Remote logging** page.

CVE-2021-34598:
If remote logging is activated, an attacker can cause a high number of events to be logged, which can lead to a system restart.

Classification of Vulnerability

CVE-2021-34582:
Base Score: 8.4
Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H

CVE-2021-34598:
Base Score: 7.5
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Temporary Fix / Mitigation

CVE-2021-34582:
If an untrusted user may have exploited the vulnerability, it is recommended to revoke access for that user, and to re-upload the certificates on the **Basic settings > LDAP** and **Logs > Remote logging** pages through the REST API (i.e., without viewing these pages in the web-based management).

CVE-2021-34598:
To prevent the possibility of an attack, it is recommended to deactivate remote logging.

Remediation

PHOENIX CONTACT recomments to upgrade to firmware version 1.5.1 (or any later version) which fixes both vulnerabitlities.

If the **Basic settings > LDAP** or **Logs > Remote logging** page are viewed after the upgrade, an exploit that may have been embedded into these pages is no longer effective.

It is recommended to review all settings for modifications that an untrusted user may have made by exploiting this vulnerability before the upgrade.

It is recommended to mistrust logs (generated before the upgrade) with respect to which user modified any settings.

Acknowledgement

CVE-2021-34582:
This vulnerability was discovered internally.

CVE-2021-34598:
This vulnerability was discovered by a key customer.
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.