

Vulnerability of FLEXLAN FX3000/2000 series and its countermeasures

■ Overview

It is found that our wireless products, FLEXLAN FX3000/2000 series, have a firmware vulnerability. There are possibilities of data plagiarism, falsification, and system destruction with malicious programs if this vulnerability was exploited by malicious attackers. The table below shows the products with a firmware vulnerability and firmware versions. This document explains the overview of this vulnerability and its countermeasures.

■ Products

Series	FLEXLAN FX3000 series		FLEXLAN FX2000 series
Model	FXA3200 FXA3000 FXA3000-US FXA3000-EU FXA3000-TW FXA3000-KR FXA3020	FXE3000 FXE3000-US FXE3000-EU FXE3000-TW FXE3000-KR FXE3000-WP FXS3000-CN FXS3001-CN	FXA2000 FXA2000-G FXA2020 FXA2300 FXE2000 FXE2000-G FXR2000 FXR2000-G
Firmware version	Below Ver.1.16.00		Below Ver.1.39.00

■ The vulnerability and its threat

For above mentioned products with listed firmware versions, we have a private webpage for developers to execute system commands, which is not linked to any other web setting pages. There are possibilities of data plagiarism, falsification, system destruction, and malicious program execution if this vulnerability was exploited by malicious attackers who can access to this private webpage (with passwords information).

■ Countermeasure

Please update a firmware to the latest version.

For FX3000 series: Ver.1.16.00 or above, for FX2000 series: Ver.1.39.00 or above.

The latest firmware is available at our website. Please type model name and find firmware.

<https://www.contec.com/download/search/>

Updated firmware is also available from a link below (software update information page):

<https://www.contec.com/software-update/2022/22082900/>

Please kindly refer to manuals or “help” on a web setting page for a firmware update procedure.

■ Workaround

If firmware cannot be updated, we highly recommend following mitigations:

- Change the password from default for accessing the product web setting page.
- Install Firewall and so on to prevent malicious access to the product's network.

■ Related Information

[JVNVU#98305100 Multiple vulnerabilities in Contec FLEXLAN FX3000 and FX2000 series](#)

■ Acknowledgement

We would like to express our gratitude to Mr. Thomas Knudsen and Mr. Samy Younsi for finding this vulnerability.

■ Contact Information

Technical Support Center <https://www.contec.com/support/technical-support/>