用於多功能小型變頻器3G3MX2 EtherNet/IPTM選配板的 NicheStack TCP/IP stack漏洞

發佈日期：2023年8月1日
台灣歐姆龍股份有限公司

■概要

歐姆龍一直致力於在工業自動化領域為客戶提供安全、可靠、高品質的產品與解決方案，這是我們立足行業，持續助推客戶業務增長，為客戶創造價值的根基。

近期，我們發現多功能小型變頻器 3G3MX2 用 EtherNet/IPTM 選配板存在多個關於 NicheStack TCP/IP stack 的漏洞。攻擊者可利用這些漏洞遠端執行代碼、干擾服務（DoS）或竊取機密資訊。

為了使您的安全得到有效保護，我們第一時間採取行動，排查受該漏洞影響的產品和版本，並推出相應對策、以及減輕措施/解決方法。您可以通過下述推薦的減輕措施/解決方法，實現將該漏洞的惡意利用風險降至最低。

■受影響產品

受本漏洞影響的產品型號及版本如下所示。

系列	型號	適用版本
MX2 EtherNet/IPTM選配板	3G3AX-MX2-EIP-A	所有版本

■漏洞內容

NicheStack TCP/IP stack漏洞

■漏洞可能造成的威脅

攻擊者可利用這些漏洞遠端執行代碼、干擾服務（DoS）或竊取機密資訊。

■CVSS 評分

DNSv4元件漏洞

長度參數不一致時處理不當（CWE-130）

CVE2020-25928

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：H/I：H/A： H 基礎評分：9.8

越界讀取（CWE-125）

CVE2020-25767

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：N/I：N/A： H 基礎評分：7.5

長度參數不一致時處理不當（CWE-130）

CVE2020-25927

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：N/I：L/A： H 基礎評分：8.2

使用不充分的隨機數（CWE-330）

CVE2021-31228

CVSS：3.1/AV：N/AC：H/PR：N/UI：N/S：C/C：N/I：L/A： N 基礎評分：4.0

使用不充分的隨機數（CWE-330）

CVE2020-25926

CVSS：3.1/AV：N/AC：H/PR：N/UI：N/S：C/C：N/I：L/A： N 基礎評分：4.0

HTTP元件漏洞

對異常情況的處理不當（CWE-703）

CVE2021-27565

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：N/I：H/A： N 基礎評分：7.5

基於堆的緩衝區溢出（CWE-122）

CVE2021-31226

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：N/I：H/A： H 基礎評分：9.1

基於堆的緩衝區溢出（CWE-122）

CVE2021-31227

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：N/I：H/A： N 基礎評分：7.5

TCP元件漏洞

異常處理不完備（CWE-248）

CVE2021-31400

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：N/I：H/A： N 基礎評分：7.5

輸入值驗證不當（CWE-20）

CVE2021-31401

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：N/I：H/A： N 基礎評分：7.5

輸入值驗證不當（CWE-20）

CVE2020-35684

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：N/I：N/A： H 基礎評分：7.5

使用不充分的隨機數（CWE-330）

CVE2020-35685

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：N/I：H/A： N 基礎評分：7.5

ICMPv4元件漏洞

輸入值驗證不當（CWE-20）

CVE2020-35683

CVSS：3.1/AV：N/AC：L/PR：N/UI：N/S：U/C：N/I：N/A： H 基礎評分：7.5

■減輕措施/解決方法

為了實現將這些漏洞的惡意利用風險降至最低，我們十分建議您採取以下減輕措施。

針對DNSv4元件漏洞

無需使用DNSv4用戶端時將其禁用。或阻斷DNSv4通信

針對 HTTP 元件漏洞

無需使用HTTP時將其禁用。或利用白名單限制HTTP連接

針對TCP元件漏洞

監控通信，攔截格式非法的TCP/IPv4數據包

針對ICMPv4元件漏洞

監控通信，攔截格式非法的ICMPv4數據包

此外，建議您採取下列常規減輕措施。

1.防病毒保護

在連接控制系統的電腦上安裝最新版本的企業級防毒軟體，並定期進行維護。

2.防止未經授權的存取

建議採取以下措施：

- 最大限度減少控制系統或設備的網路連接，禁止不受信任的設備存取
- 通過部署防火牆隔離 IT 網路（斷開未使用的通訊端口、限制通訊主機）
- 需要遠程存取控制系統或設備時，使用虛擬專用網路（VPN）
- 使用高強度密碼並定期更換
- 引入實體控制，確保只有授權人員才能存取控制系統和設備
- 在控制系統或設備中使用 USB 儲存器等外部儲存設備時，先進行病毒掃描
- 遠程存取控制系統或設備時，實施多重驗證

3.數據輸入/輸出保護

確認備份和範圍檢查等設置的合理性，以防止對控制系統和設備的輸入/輸出數據進行意外修改。

4.恢復丟失的數據

定期對設置數據進行備份和維護，以防數據丟失。

■諮詢方式

如您在採取減輕措施/解決方案時遇到問題，可以透過以下方式聯繫歐姆龍營業據點或經銷商：

https://www.ia.omron.com/global_network/index.html

■更新記錄

2023年8月1日 創建