多機能型小型インバータ 3G3MX2 用 EtherNet/IP™ オプションボードにおける、NicheStack TCP/IP stack の脆弱性

公開日 2023 年 8 月 1 日

オムロン株式会社

■概要

多機能型小型インバータ 3G3MX2 用 EtherNet/IP™ オプションボードにおいて NicheStack TCP/IP stack に関する複数の脆弱性が存在することが判明しました。

攻撃者はこの脆弱性を利用し、リモートコード実行やサービス妨害（DoS）、機微な情報を窃取できる可能性があります。

この脆弱性の影響を受ける製品、バージョン、および軽減策・回避方法を以下に示します。弊社が推奨する軽減策・回避策を実施することで、本脆弱性の悪用リスクを最小限に抑えることができます。

■対象製品

本脆弱性の影響を受ける製品の形式、およびバージョンは以下の通りです。

シリーズ	形式	対象バージョン
MX2 EtherNet/IP™ Option Board	3G3AX-MX2-EIP-A	全て

■脆弱性内容

NicheStack TCP/IP stack の脆弱性

■脆弱性により想定される脅威

攻撃者はこの脆弱性を利用し、リモートコード実行やサービス妨害（DoS）、機微な情報を窃取できる可能性があります。

■CVSS スコア

DNSv4 コンポーネントの脆弱性

長さパラメータ不整合時の不適切な取り扱い (CWE-130)

CVE2020-25928

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H　基本値: 9.8

境界外読み取り (CWE-125)

CVE2020-25767

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H　基本値: 7.5

長さパラメータ不整合時の不適切な取り扱い (CWE-130)

CVE2020-25927

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H　基本値: 8.2

不十分なランダム値の使用 (CWE-330)
CVE2021-31228
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N 基本値: 4.0
不十分なランダム値の使用 (CWE-330)
CVE2020-25926
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N 基本値: 4.0

HTTP コンポーネントの脆弱性
不適切な例外条件の処理 (CWE-703)
CVE2021-27565
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値: 7.5
ヒープベースのバッファオーバーフロー (CWE-122)
CVE2021-31226
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H 基本値: 9.1
ヒープベースのバッファオーバーフロー (CWE-122)
CVE2021-31227
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値: 7.5

TCP コンポーネントの脆弱性
例外処理の不備 (CWE-248)
CVE2021-31400
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値: 7.5
不適切な入力値検証 (CWE-20)
CVE2021-31401
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値: 7.5
不適切な入力値検証 (CWE-20)
CVE2020-35684
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値: 7.5
不十分なランダム値の使用 (CWE-330)
CVE2020-35685
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値: 7.5

ICMPv4 コンポーネントの脆弱性
不適切な入力値検証 (CWE-20)
CVE2020-35683
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値: 7.5

■軽減策・回避策

本脆弱性の悪用リスクを最小限に抑えるため、以下に示す軽減策を講じることを推奨します。

DNSv4 コンポーネントの脆弱性に対して

必要のない場合は DNSv4 クライアントを無効化する。または DNSv4 通信をブロックする

HTTP コンポーネントの脆弱性に対して

必要のない場合は HTTP を無効化する。または、ホワイトリストを用いて HTTP 接続を制限する

TCP コンポーネントの脆弱性に対して

通信をモニタリングし、不正な形式の TCP/IPv4 パケットをブロックする

ICMPv4 コンポーネントの脆弱性に対して

通信をモニタリングし、不正な形式の ICMPv4 パケットをブロックする

また、以下に示す一般的な軽減策も推奨します。

1. アンチウィルス保護

制御システムに接続するパソコンに最新の商用品質のウイルス対策ソフトの導入・保守

2. 不正アクセスの防止

- 制御システムや装置のネットワーク接続を最小限に抑え、信頼できないデバイスからのアクセス禁止
- ファイアウォールの導入による IT ネットワークからの分離（未使用通信ポートの遮断、通信ホストの制限）
- 制御システムや装置へのリモートアクセスが必要な場合、仮想プライベートネットワーク（VPN)の使用
- 強固なパスワードの採用と頻繁な変更
- 権限保有者のみを制御システムや装置へのアクセスを可能とする物理的統制の導入
- 制御システムや装置で USB メモリなど外部ストレージデバイスを使用する場合の事前ウイルススキャン
- 制御システムや装置へのリモートアクセス時の多要素認証の導入

3. データ入出力の保護

制御システムや装置への入出力データの意図せぬ改変に備えた、バックアップや範囲チェックなどの妥当性の確認

4. 紛失データの復元

データ紛失対策としての定期的な設定データのバックアップと保守

■お問い合わせ先

当社営業または販売店にお問い合わせください。

国内お問い合わせ先：https://www.fa.omron.co.jp/sales/local/

海外お問い合わせ先：https://www.ia.omron.com/global_network/index.html

■更新履歴

2023/8/1 新規作成