NicheStack TCP/IP stack Vulnerabilities on EtherNet/IP™ option board for Multi-function Compact Inverter 3G3MX2

Release date: August 1, 2023
OMRON Corporation

■ Overview
Vulnerabilities related to NicheStack TCP/IP stack exist in the EtherNet/IP™ option board for Multi-function Compact Inverter 3G3MX2.
An attacker may use these vulnerabilities to perform remote code execution, denial of service (DoS), or obtain sensitive information.
The products and versions affected by these vulnerabilities, mitigation and protection measures are shown below. Make sure to implement these recommended mitigations and protections to minimize the risk of exploitation of these vulnerabilities.

■ Affected products
Affected products and versions are below.

<table>
<thead>
<tr>
<th>Product series</th>
<th>Model</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MX2 EtherNet/IP™ Option Board</td>
<td>3G3AX-MX2-EIP-A</td>
<td>All versions</td>
</tr>
</tbody>
</table>

■ Description
Vulnerabilities related to NicheStack TCP/IP stack

■ Potential threats and impacts
An attacker may use these vulnerabilities to perform remote code execution, denial of service (DoS), or obtain sensitive information.

■ CVSS Scores
DNSv4 component vulnerability
Improper Handling of Length Parameter Inconsistency (CWE-130)
CVE2020-25928
Out-of-bounds Read (CWE-125)
CVE2020-25767
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score: 7.5

Improper Handling of Length Parameter Inconsistency (CWE-130)
CVE2020-25927
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H Base Score: 8.2

Use of Insufficiently Random Values (CWE-330)
CVE2021-31228
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N Base Score: 4.0

HTTP component vulnerability
Improper Check or Handling of Exceptional Conditions (CWE-703)
CVE2021-27565

Heap-based Buffer Overflow (CWE-122)
CVE2021-31226
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H Base Score: 9.1

TCP component vulnerability
Uncaught Exception (CWE-248)
CVE2021-31400

Improper Input Validation (CWE-20)
CVE2021-31401

Improper Input Validation (CWE-20)
CVE2020-35684
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score: 7.5

Use of Insufficiently Random Values (CWE-330)
CVE2020-35685
ICMPv4 component vulnerability
Improper Input Validation (CWE-20)
CVE2020-35683
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score: 7.5

Mitigations and Protections
OMRON recommends that customers take the following mitigation measures to minimize the risk of exploitation of these vulnerabilities.

For vulnerabilities in DNSv4 components
   Disable DNSv4 clients or block DNSv4 communication if not needed.
For vulnerabilities in HTTP component
   Disable HTTP if not needed. Or use a whitelist to limit HTTP connections.
For vulnerabilities in TCP components
   Monitor communications and block malformed TCP/IPv4 packets.
For vulnerabilities in ICMPv4 components
   Monitor communications and block malformed TCP/IPv4 packets.

OMRON also recommends the following general mitigation measures.

1. Anti-virus protection
   - Protect any PC with access to the control system against malware and ensure installation and maintenance of up-to-date commercial grade anti-virus software protection

2. Security measures to prevent unauthorized access
   - Minimize connection of control systems and equipment to open networks, so that untrusted devices will be unable to access them.
   - Implement firewalls (by shutting down unused communications ports, limiting communications hosts) and isolate them from the IT network.
   - Use a virtual private network (VPN) for remote access to control systems and equipment.
   - Use strong passwords and change them frequently.
   - Install physical controls so that only authorized personnel can access control systems and equipment.
   - Scan virus to ensure safety of any USB drives or similar devices before connecting them to systems and devices.
   - Enforce multifactor authentication to all devices with remote access to control systems and equipment whenever possible.
3. Data input and output protection
   • Validation processing such as backup and range check to cope with unintentional modification of input/output data to control systems and devices.
4. Data recovery
   • Periodical data backup and maintenance to prepare for data loss

Contact information
Please contact our sales office or distributors.

Update history
- August 1, 2023: New Release