用于多功能小型变频器 3G3MX2 EtherNet/IP™ 选配板的 NicheStack TCP/IP stack 漏洞

发布日期：2023 年 8 月 1 日

欧姆龙株式会社

■概要

欧姆龙一直致力于在工业自动化领域为客户提供安全、可靠、高质量的产品与解决方案，这是我们立足行业，持续助推客户业务增长，为客户创造价值的根基。

近期，我们发现多功能小型变频器 3G3MX2 用 EtherNet/IP™ 选配板存在多个关于 NicheStack TCP/IP stack 的漏洞。

攻击者可利用这些漏洞远程执行代码、干扰服务（DoS）或窃取机密信息。

为了使您的安全得到有效保护，我们第一时间采取行动，排查受该漏洞影响的产品和版本，并推出相应对策、以及减轻措施/解决方法。您可以通过下述推荐的减轻措施/解决方法，实现将该漏洞的恶意利用风险降至最低。

■对象产品

受这些漏洞影响的产品型号及版本如下所示。

系列	型号	适用版本
MX2 EtherNet/IP™ 选配板	3G3AX-MX2-EIP-A	所有版本

■漏洞内容

NicheStack TCP/IP stack 漏洞

■漏洞可能造成的威胁

攻击者可利用这些漏洞远程执行代码、干扰服务（DoS）或窃取机密信息。

■CVSS 评分

DNSv4 组件漏洞

长度参数不一致时处理不当（CWE-130）

CVE2020-25928

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 基础评分：9.8

越界读取（CWE-125）

CVE2020-25767

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基础评分：7.5

长度参数不一致时处理不当（CWE-130）

CVE2020-25927

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H 基础评分：8.2

使用不充分的随机数（CWE-330）

CVE2021-31228

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N 基础评分：4.0

使用不充分的随机数（CWE-330）

CVE2020-25926

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N 基础评分：4.0

HTTP 组件漏洞

对异常情况的处理不当（CWE-703）

CVE2021-27565

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基础评分：7.5

基于堆的缓冲区溢出（CWE-122）

CVE2021-31226

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H 基础评分：9.1

基于堆的缓冲区溢出（CWE-122）

CVE2021-31227

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基础评分：7.5

TCP 组件漏洞

异常处理不完备（CWE-248）

CVE2021-31400

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基础评分：7.5

输入值验证不当（CWE-20）

CVE2021-31401

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基础评分：7.5

输入值验证不当（CWE-20）

CVE2020-35684

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基础评分：7.5

使用不充分的随机数（CWE-330）

CVE2020-35685

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N 基础评分：7.5

ICMPv4 组件漏洞

输入值验证不当（CWE-20）

CVE2020-35683

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基础评分：7.5

■减轻措施/解决方法

为了实现将这些漏洞的恶意利用风险降至最低，我们十分建议您采取以下减轻措施。

针对 DNSv4 组件漏洞

无需使用 DNSv4 客户端时将其禁用。或阻断 DNSv4 通信

针对 HTTP 组件漏洞

无需使用 HTTP 时将其禁用。或利用白名单限制 HTTP 连接

针对 TCP 组件漏洞

监控通信，拦截格式非法的 TCP/IPv4 数据包

针对 ICMPv4 组件漏洞

监控通信，拦截格式非法的 ICMPv4 数据包

此外，还推荐采取下列常规减轻措施。

1. 防病毒保护

在连接控制系统的电脑上安装最新版本的企业级杀毒软件，并定期维护。

2. 防止未经授权的访问

- 最大限度地减少控制系统或设备的网络连接，禁止不受信任的设备访问
- 通过部署防火墙隔离 IT 网络（断开未使用的通信端口、限制通信主机）
- 需要远程访问控制系统或设备时，使用虚拟专用网络（VPN）
- 使用高强度密码并定期修改
- 引入物理控制，确保仅授权人员可访问控制系统和设备
- 在控制系统或设备中使用 USB 存储器等外部存储设备时，事先进行病毒扫描
- 在远程访问控制系统或设备时进行多重要素验证

3. 数据输入/输出保护

确认备份和范围检查等设置的合理性，以防对控制系统和设备的输入/输出数据的意外修改

4. 恢复丢失的数据

定期对设置数据进行备份和维护，以防数据丢失

■咨询方式

如您在采取减轻措施/解决方法时遇到问题，可以通过下列方式向我们的事务所或经销商咨询：

https://www.fa.omron.com.cn/contactus

■更新记录

2023 年 8 月 1 日创建