

Product Cybersecurity Advisory
(产品网络安全公告)

CANOpen Builder 存在二进制漏洞的处置建议

June 21, 2024

Purpose (目的)

台达电子于 2024 年 1 月 19 日收到 CNVD 通知产品 CANOpen Builder 6.07 存在二进制漏洞，在此针对漏洞的相关分析处理、安排及缓解方案提出说明。

Vulnerabilities Details (漏洞详情)

#	Vulnerability Type 漏洞类型	Severity 严重性	Impact 影响
1	CWE-823 Use of Out-of-range Pointer Offset	High	攻击者可引导用户打开恶意的工程文件，程序访问了非法地址，导致程序崩溃。

Affected Products (受影响的产品)

Product Series 产品系列	Affected Versions 受影响版本
CANOpen Builder	V6.07 及之前版本

Mitigations (缓解方案)

Product Series 产品系列	Mitigations 缓解方案	Notifications 注意事项
CANOpen Builder	请下载并更新至 CANOpen Builder v6.09 或之后版本。 請至官網下載：https://downloadcenter.delta-china.com.cn/zh-CN/DownloadCenter?v=1&q=canopen&sort_expr=cdate&sort_dir=DESC	无

Acknowledgements (致谢)

台达电子非常感谢 CNVD 发现并报告该漏洞，协助我们提高产品的安全性，并帮助我们为客户提供更好的服务。

Contact Us (联络信息)

我们对产品秉持高度重视，非常欢迎您向我们提出产品网络安全问题。台达电子将持续监控已知和未知的威胁，积极主动地面对新的产品网络安全问题，作为支持台达产品网络安全的基础。

如果您有任何产品相关问题，请透过以下公司连结找到联系窗口，以获取您可能需要的信息或信息

- 繁体中文：https://www.deltaww.com/zh-TW/Customer-Service
- 简体中文：https://www.delta-china.com.cn/zh-CN/customerService_Products

We appreciate and value having cybersecurity concerns brought to our attention. Delta Electronics constantly monitors for both known and unknown threats. Being proactive rather than reactive to emerging security issues is fundamental for product support at Delta Electronics.

If you have any product-related support concerns, please find a contact from the following company's portal page to reach us for any information or materials you may require.

- https://www.deltaww.com/en-US/Customer-Service

Term of Use (使用条款)

请透过以下连结获取更多获取更多使用条款之适用范围信息。

Please visit the link below for more information on the scope of terms of use.

- English：https://www.deltaww.com/en-US/information/Terms-of-use
- 繁体中文：https://www.deltaww.com/zh-TW/information/Terms-of-use
- 简体中文：https://www.delta-china.com.cn/zh-CN/information/Terms-of-use

Revision History (修订记录)

Release Date 发布尔日期	Revision 版本	Description 说明
January 31, 2024	1.0	First publication