Product Cybersecurity Advisory

COMMGR

Stack-based Buffer Overflow and Code Injection Vulnerabilities

1. Summary (总结/總結)

Published Date (发布/發布)	August 26, 2025	**Last Updated (最后更新/最後更新)**	August 26, 2025
Severity (严重度/嚴重度)	High	**CVSS**	(v3) 8.6
Product (产品/產品)	COMMGR		
Vulnerability (漏洞)	Stack-based Buffer Overflow and Code Injection Vulnerabilities		
Corrected (修正)	Corrected	**Workaround (权宜措施/權宜措施)**	No

2. Affected Products (受影响产品/受影響產品)

Product (产品/產品)	Version (版本/版本)
COMMGR	V2.9.0 and prior

3. Vulnerability Overview (漏洞概述/漏洞概述)

#	Type (类型/類型)	Severity	CVE ID	Related Link (相关链接/相關連結)
1	CWE-121 Stack-based Buffer Overflow	High	CVE-2025-53418	
2	CWE-94 Code Injection	High	CVE-2025-53419	

4. Mitigations (缓解/緩解)

Product (产品/產品)	Mitigations (缓解/緩解)	Download Link (下载连结/下載連結)
COMMGR	➢ Download and update to: v2.10.0 or later ➢ 下载并更新至: v2.10.0 (或更新的版本) ➢ 下載並更新至: v2.10.0 (或更新的版本)	➢ Delta Download Center ➢ 台达下载中心

5. General Recommendations (一般性建议/一般性建議)

A. Don’t click on untrusted Internet links or open unsolicited attachments in emails.
不要点击无法信任的网络链接，或打开电子邮件中未经请求的附件。
不要點擊無法信任的網路連結，或打開電子郵件中未經請求的附件。

B. Avoid exposing control systems and equipment to the Internet.
避免让控制系统及设备暴露于因特网 (Internet) 上。
避免讓控制系統及設備暴露於網際網路 (Internet) 上。

C. Place systems and devices behind a firewall and isolate them from the business network.
请将系统与设备置于防火墙之后，并将它们与业务网络 (business network) 隔离。
請將系統與設備置於防火牆之後，並將它們與業務網路 (business network) 隔離。

D. When remote access is required, use a secure access method, such as a virtual private network (VPN).
需要远程访问时，要使用安全的访问方式，例如：虚拟专用网络 (VPN)。
需要遠程訪問時，要使用安全的訪問方式，例如：虛擬專用網路 (VPN)。

6. Contact Us (联络我们/聯絡我們)

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

If you have any product-related support concerns, please find a contact from the above company's portal page to reach us for any information or materials you may require.
如果有任何与产品相关的问题，请从上面入口网页找到联络人，以便取得您需要的任何信息。
如果有任何與產品相關的問題，請從上面入口網頁找到聯絡人，以便取得您需要的任何資訊。

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.
台达电子重视网络安全问题，并不断监控已知和未知的威胁。主动而非被动地应对新出现的安全问题是台达电子产品支持的基础。
台達電子重視網路安全問題，並不斷監控已知和未知的威脅。主動而非被動地應對新出現的安全問題是台達電子產品支援的基礎。

7. Term of Use (使用条款/使用條款)

- 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

- 请访问下面的链接，以了解有关使用条款范围的更多信息。
  简体中文：https://www.delta-china.com.cn/zh-CN/information/Terms-of-use

- 請訪問下面的連結，以了解有關使用條款範圍的更多資訊。
  繁體中文：https://www.deltaww.com/zh-TW/information/Terms-of-use