Product Cybersecurity Advisory

DVP12SE – Multiple Vulnerabilities

1. Summary (总结/總結)

Revision	V1.0	**Last Revised**	2026-06-30	**Initial Release**	2026-06-30
Product (产品/產品)		DVP12SE		**Severity (严重度/嚴重度)**	Critical
Corrected (修正)		No		**Workaround (权宜措施/權宜措施)**	Yes

2. Affected Products (受影响产品/受影響產品)

Product (产品/產品)	Version (版本/版本)
DVP12SE	ALL

3. Vulnerability Overview (漏洞概述/漏洞概述)

#	Type (类型/類型)	Severity	CVE ID	CVSS	CVSS Vector String
1	CWE-770 Allocation of Resources Without Limits or Throttling	Critical	CVE-2026-12818	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2	CWE-306 Missing Authentication for Critical Function	Critical	CVE-2026-12819	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

4. Workaround (权宜措施/權宜措施)

Product (产品/產品)	Workaround (权宜措施/權宜措施)	Download Link (下载连结/下載連結)
DVP12SE	English Users are recommended to take the following mitigation measures: ➢ Enable the IP Filter feature: Configure and enable the PLC's built-in IP Filter function via the programming software. Restrict access exclusively to the IP addresses of trusted devices (such as designated HMI panels or SCADA hosts) to block unauthorized network access. ➢ Set up PLC password protection: Enable password protection for the PLC within the programming software to ensure the device's core control logic and parameters cannot be easily downloaded, overwritten, or tampered with. ➢ Implement network isolation and firewall protection: Deploy the PLC within an independent local area network (OT control network) secured by a firewall. Never connect the device directly to the office network or the Internet. If remote access is required, enforce the use of a secure, authorized VPN tunnel. For other general practices, please refer to the precautions in the General Recommendations. 简中 建议使用者采取以下缓解措施: ➢ 启用 IP 过滤功能 (IP Filter): 请透过工程软件开启 PLC 内建的 IP 过滤功能，仅允许信任的设备（如指定的 HMI 监控画面或 SCADA 主机）之 IP 地址联机至 PLC，以直接阻绝未授权的网络存取。 ➢ 设定 PLC 密码保护: 请在工程软件中为 PLC 设定密码保护，确保设备的核心控制逻辑与参数不会被轻易下载、覆写或窜改。 ➢ 实施网络物理隔离与防火墙防护: 请架设具有防火墙的独立局域网络（OT 控制网络）来部署 PLC，切勿将设备直接连接至可连外网的办公网络或因特网。若需远程联机，请强制透过公司核准的安全 VPN 通道进行。 其余请参考 General Recommendations 中的注意事项。 繁中 建議使用者採取以下緩解措施： ➢ 啟用 IP 過濾功能 (IP Filter)： 請透過工程軟體開啟 PLC 內建的 IP 過濾功能，僅允許信任的設備（如指定的 HMI 監控畫面或 SCADA 主機）之 IP 位址連線至 PLC，以直接阻絕未授權的網路存取。 ➢ 設定 PLC 密碼保護： 請在工程軟體中為 PLC 設定密碼保護，確保設備的核心控制邏輯與參數不會被輕易下載、覆寫或竄改。 ➢ 實施網路物理隔離與防火牆防護： 請架設具有防火牆的獨立區域網路（OT 控制網路）來部署 PLC，切勿將設備直接連接至可連外網的辦公網路或網際網路。若需遠端連線，請強制透過公司核准的安全 VPN 通道進行。 其餘請參考 General Recommendations 中的注意事項。	

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. Acknowledgements (致谢/致謝)

Delta Electronics would like to thank CISA for their assistance in coordinating this disclosure, and Adm Bin Harbi (0xnoag) - Corvo Security for reporting this vulnerability.

台达电子衷心感谢 CISA 在本漏洞揭露过程中的协助与协调，并感谢 Adm Bin Harbi (0xnoag) - Corvo Security 通报此漏洞。

台達電子衷心感謝 CISA 在本漏洞揭露過程中的協助與協調，並感謝 Adm Bin Harbi (0xnoag) - Corvo Security 通報此漏洞。

7. 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。

8. 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