Product Cybersecurity Advisory

DOPSoft 4 EOL – Cybersecurity Advisory

October 23, 2023

Purpose:

DOPSoft 4 was officially end-of-life on October 23, 2023 (the last version is v4.00.16.30). Delta Electronics has discontinued the maintenance of DOPSoft 4.

After the end-of-life (EOL), no security vulnerabilities, whether known or unknown, will be patched. Using DOPSoft 4 may pose security risks.

Users who continue using DOPSoft 4 shall take proper security precautions in the usage environment (please refer to the 'Security Recommendations for Usage' below). And it is strongly recommended that users switch to "DIAScreen HMI Programming Software."

If users want to continue using it, please pay attention to strengthening the safety protection of the use environment (please refer to the "Safety Usage Recommendations" below), and strongly recommend that users switch to "DIAScreen Human Machine Interface Programming Software". "DIAScreen 人機界面程式設計軟體"。

Security Recommendations for Usage:

- It is highly recommended to switch to "DIAScreen HMI Programming Software" immediately.
- When using software products, please ensure the following:
  1. Place the software and devices behind a firewall and isolate them from the business network.
  2. Use secure access channel, such as a Virtual Private Network (VPN), when remote access is required.
  3. Store user-created files in a secure storage location and grant file access permissions only to trusted users.
  4. Do not run the software with administrator privileges to prevent copying files from critical system folders.
  5. Do not connect the programming software to any network other than the device's private network.
  6. Keep your operating system up to date. Ensure that the operating system and related software are the latest versions.
  7. Do not click on untrusted web links or open unsolicited email attachments.

Know Vulnerabilities: (DOPSoft v4.00.16.22 and later)

#	Vulnerability Type	Severity	Influence
1	Stack-based Buffer Overflow	High	The Stack-based Buffer Overflow (CWE-121) vulnerability can be exploited by processing a specially crafted project file, which could allow an attacker to execute arbitrary code.
	Base Score：7.8 (CVSS v3.1) Vector：AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		
2	Out-Of-Bounds Write	Hign	The Out-Of-Bounds Write (CWE-787) vulnerability can be exploited by processing a specially crafted project file, which could allow an attacker to execute arbitrary code.
	Base Score：7.8 (CVSS v3.1) Vector：AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		

If you have any security question about products, please use the following link to find the contact window for information you may need:

- https://www.deltaww.com/en-US/customerService_Products

Revision History:

Publish Date	Version	Description
October 23, 2023	1.0	First publication