Product Cybersecurity Advisory

DTM Soft Deserialization of Untrusted Data Vulnerability

August 8, 2024

Purpose

Delta Electronics received a notification from ICS-CERT on March 4, 2024 that the product DTMSoft (v1.30) has deserialization of untrusted data vulnerability. Here we provide instructions on the relevant analysis, processing, arrangements and mitigation plans for the vulnerability.

Vulnerabilities Details

#	Vulnerability Type	CVE Number	Severity	Impact
1	Deserialization of Untrusted Data (CWE-502)	CVE-2024-xxxxx (TBD)	High	An attacker can create a malicious data file and cause arbitrary code execution when the data is deserialized.

Affected Products

Product Series	Affected Versions
DTM Soft	V1.30 and prior

Solutions

Product Series	Solutions	Notifications
DTM Soft	Delta Electronics is actively patching this vulnerability and expects to release a new version at the end of September 2024. This advisory will be updated in due course, and users are recommended to download and update to the latest version from Delta's official website then.	

Mitigations

Product Series	Mitigations	Notifications

DTM Soft	Before Delta provides a patched version, users are advised to pay attention to the followings to reduce risks: ➢ Store user created files in a secure storage location and limit access to the files to only trusted users. ➢ Start the software without administrator rights to prevent the copying of extracted files in critical system folders.. ➢ For all methods of mobile data exchange (e.g. CDs, USB drives, etc.), scan them with the isolated network before use in the terminals or any node connected to these networks. ➢ To stay informed of all updates, including details on affected products and remediation plans. ➢ Minimize network exposure for all control system devices and software, and ensure they are not accessible from the Internet. ➢ When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). ➢ Locate control system networks and remote devices behind firewalls and isolate them from the business network.	None

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

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
➢ Traditional Chinese: https://www.deltaww.com/zh-TW/information/Terms-of-use
➢ Simplified Chinese: https://www.delta-china.com.cn/zh-CN/information/Terms-of-use

Revision History

Release Date	Revision	Description
August 8, 2024	1.0	First publication