



CVE-2022-1370

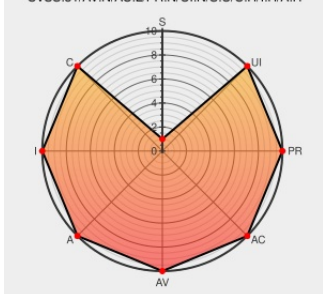
Published on: Not Yet Published

Last Modified on: 05/10/2022 07:47:00 PM UTC

CVE-2022-1370 - advisory for ICSA-22-081-01

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Diaenergie](#) from [Deltaww](#) contain the following vulnerability:

Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in ReadREGbyID. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.

CVE-2022-1370 has been assigned by [ics-cert@hq.dhs.gov](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Delta Electronics](#) - **DIAEnergie** version < 1.8.02.004

Vulnerability Patch/Work Around

Delta also suggests users: Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet. Locate control system networks and remote devices behind firewalls and isolate them from the business network. Use an application firewall that can detect attacks against "Path Traversal" and "SQL Injection" weakness. Never connect programming software to any network other than the network intended for that device. When remote access is required, use secure methods, such as virtual private networks (VPNs), recognizing a VPN is only as secure as its connected devices

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

