

CVE-2021-38406

Delta Electronics DOPSoft 2 Improper Input Validation Vulnerability

CISA KEV since Aug 25, 2022

Actively exploited

Delta Electronic DOPSoft 2 (Version 2.00.07 and prior) lacks proper validation of user-supplied data when parsing specific project files. This could result in multiple out-of-bounds write instances. An attacker could leverage this vulnerability to execute code in the context of the current process.

EVRS 78/₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.764 99.54th percentile · FIRST	CISA DEADLINE Sep 15, 2022 KEV since 2022 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.764 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: The impacted product is end-of-life and should be disconnected if still in use.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
dopsoft	≥ 2.00 ≤ 2.00.07	after 2.00.07	NVD

Sources

Vendor guidance github.com/advisories/GHSA-j3xh-c39x-qghw
NVD nvd.nist.gov/vuln/detail/CVE-2021-38406
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2021-24858

cisa.gov cisa.gov/uscrt/ics/advisories/icsa-21-252-02
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2021-38406

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.