ASDA-Soft Stack-based Buffer Overflow Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-5726
State	PUBLISHED
Assigner	Deltaww
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 03:16:07 UTC
Updated	2026-04-13 12:49:03 UTC
Description	ASDA-Soft Stack-based Buffer Overflow Vulnerability

Risk And Classification

Primary CVSS: v3.1 8.4 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000050000 probability, percentile 0.002520000 (date 2026-04-15)

Problem Types: CWE-121 | CWE-787 | CWE-121 CWE-121 Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	759f5e80-c8e1-4224-bead-956d7b33c98b	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Deltaww	Asda Soft	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	DeltaWW	ASDA-Soft	affected 7.2.2.0 custom	Windows

References

Reference	Source
filecenter.deltaww.com/news/download/doc/Delta-PCSA-2026-00007_ASDA-Soft%20Stack-bas...	759f5e80-c8e1-4224-bead-956d7b33c98
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: CISA (en)

CNA: Zero Day Initiative (ZDI) (en)

Additional Advisory Data

Solutions

CNA: Download and update to: ASDA-Soft v7.2.6.0 or later (Delta Download Center)

There are currently no legacy QID mappings associated with this CVE.

site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report