



Heap-based Buffer Overflow in Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, Cobalt Share

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2025-65085
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-11-25 18:15:54 UTC
Updated	2026-05-12 21:16:13 UTC
Description	A Heap-based Buffer Overflow vulnerability is present in Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share ve

Risk And Classification

Primary CVSS: v4.0 8.4 HIGH from ics-cert@hq.dhs.gov

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.001230000 probability, percentile 0.309290000 (date 2026-05-12)

Problem Types: CWE-122 | CWE-122 CWE-122 Heap-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/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	Ashlar	Argon	All	All	All	All
Application	Ashlar	Cobalt	All	All	All	All
Application	Ashlar	Cobalt Share	All	All	All	All
Application	Ashlar	Lithium	All	All	All	All

Application	Ashlar	Xenon	All	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Ashlar-Vellum	Cobalt	affected 12.6.1204.216 custom	Not specified		
CNA	Ashlar-Vellum	Xenon	affected 12.6.1204.216 custom	Not specified		
CNA	Ashlar-Vellum	Argon	affected 12.6.1204.216 custom	Not specified		
CNA	Ashlar-Vellum	Lithium	affected 12.6.1204.216 custom	Not specified		
CNA	Ashlar-Vellum	Cobalt Share	affected 12.6.1204.216 custom	Not specified		
References						
Reference	Source	Link	Tags			
www.cisa.gov/news-events/ics-advisories/icsa-25-329-01	ics-cert@hq.dhs.gov	www.cisa.gov	Third Party Advisory, US Government Res			
CVE Program record	CVE.ORG	www.cve.org	canonical			
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis			
Vendor Comments And Credit						
Discovery Credit						
CNA: Michael Heinzl reported these vulnerabilities to CISA. (en)						
Additional Advisory Data						
Solutions						
CNA: Ashlar-Vellum recommends users update to build 12.6.1204.217 and later.						
There are currently no legacy QID mappings associated with this CVE.						

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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