



# Out-of-bounds Write in Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, Cobalt Share

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

## Summary

<b>CVE</b>	CVE-2025-65084
<b>State</b>	PUBLISHED
<b>Assigner</b>	icscert
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-11-25 18:15:54 UTC
<b>Updated</b>	2026-05-12 21:16:13 UTC
<b>Description</b>	An Out-of-Bounds Write vulnerability is present in Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share versions

## 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:** 0.001670000 probability, percentile 0.373480000 (date 2026-05-12)

**Problem Types:** CWE-787 | CWE-787 CWE-787 Out-of-bounds Write

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
<b>Vendor Declared Affected Products</b>						
Source	Vendor	Product	Version	Platforms		
CNA	<a href="#">Ashlar-Vellum</a>	<a href="#">Cobalt</a>	affected 12.6.1204.216 custom	Not specified		
CNA	<a href="#">Ashlar-Vellum</a>	<a href="#">Xenon</a>	affected 12.6.1204.216 custom	Not specified		
CNA	<a href="#">Ashlar-Vellum</a>	<a href="#">Argon</a>	affected 12.6.1204.216 custom	Not specified		
CNA	<a href="#">Ashlar-Vellum</a>	<a href="#">Lithium</a>	affected 12.6.1204.216 custom	Not specified		
CNA	<a href="#">Ashlar-Vellum</a>	<a href="#">Cobalt Share</a>	affected 12.6.1204.216 custom	Not specified		
<b>References</b>						
Reference	Source	Link	Tags			
<a href="http://www.cisa.gov/news-events/ics-advisories/icsa-25-329-01">www.cisa.gov/news-events/ics-advisories/icsa-25-329-01</a>	<a href="mailto:ics-cert@hq.dhs.gov">ics-cert@hq.dhs.gov</a>	<a href="http://www.cisa.gov">www.cisa.gov</a>	Third Party Advisory, US Government Res			
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical			
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis			
<b>Vendor Comments And Credit</b>						
Discovery Credit						
<b>CNA:</b> Michael Heinzl reported these vulnerabilities to CISA. (en)						
<b>Additional Advisory Data</b>						
Solutions						
<b>CNA:</b> 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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)