



CVE-2022-0835

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

Summary

CVE	CVE-2022-0835
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-11 20:15:00 UTC
Updated	2022-04-18 13:42:00 UTC
Description	AVEVA System Platform 2020 stores sensitive information in cleartext, which may allow access to an attacker or a low-priv

Risk And Classification

Problem Types: CWE-312

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aveva	System Platform	2020	-	All	All
Application	Aveva	System Platform	2020	r2s	All	All
Application	Aveva	System Platform	2020	r2_patch01	All	All

References

Reference	Source	Link	Tags
www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/Se...	CONFIRM	www.aveva.com	
AVEVA System Platform CISA	CONFIRM	www.cisa.gov	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Noam Moshe of Claroty and Ilya Karpov, Evgeniy Druzhinin, and Konstantin Kondratev of Rostelecom-Solar reported this vulnerability to AVEVA.

Legacy QID Mappings

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web 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](#)