DATE: 09/08/2021

SECURITY BULLETIN AVEVA-2021-008

Title

DLL Hijacking through Uncontrolled Search Path Element in the PCS Portal Application

Rating

High

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. ("AVEVA") has created security updates to address DLL Hijacking vulnerabilities in the Platform Common Services (PCS) Portal versions 4.5.2, 4.5.1, 4.5.0, and 4.4.6. The vulnerabilities, if exploited, could allow malicious code execution within the context of the PCS Portal application.

The following products ship a vulnerable version of the PCS Portal application and are affected:

- AVEVA™ System Platform 2020 R2 P01, 2020 R2, and 2020
- AVEVA™ Work Tasks 2020 Update 1
- AVEVA™ Work Tasks 2020
- AVEVA™ Mobile Operator 2020
- AVEVA™ Manufacturing Execution System 2020
- AVEVA™ Batch Management 2020
- AVEVA™ Enterprise Data Management 2021

Recommendations

AVEVA recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

Customers using affected versions of the products should apply the corresponding security update as soon as possible:

Version	Security Update	Download Link
AVEVA™ Mobile Operator 2020 AVEVA™ Enterprise Data Management 2021 AVEVA™ System Platform 2020 R2 P01 AVEVA™ System Platform 2020 R2 AVEVA™ Work Tasks 2020 Update 1	PCS 4.5.3	https://softwaresupportsp.aveva.com/#/producthub/details?id=5091eef4-db87-4a32-024b-08d9609a6c7a

Version	Security Update	Download Link
AVEVA™ System Platform 2020 AVEVA™ Work Tasks 2020 AVEVA™ Manufacturing Execution System 2020 AVEVA™ Batch Management 2020	PCS 4.4.7	https://softwaresupportsp.aveva.com/#/producthub/details?id=e4563524-e7cf-4c53-024a-08d9609a6c7a

Vulnerability Characterization and CVSSv3 Rating

CWE-427: DLL Hijacking through Uncontrolled Search Path Element
PCS Portal: **7.3** | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Acknowledgements

AVEVA would like to thank:

- **Noam Moshe of Claroty** for the discovery and responsible disclosure of this vulnerability
- **ICS-Cert** for coordination of advisories

Support

For information on how to reach AVEVA support for your product, please refer to this link: AVEVA Customer Support.
If you discover errors or omissions in this Security Notification, please report the finding to Support.

AVEVA Security Central

For the latest security information and security updates, please visit Security Central.

Cyber Security Standards and Best Practices

For information regarding how to secure Industrial Control Systems please reference NIST SP800-82r2.

NVD Common Vulnerability Scoring System (CVSS v3)

The U.S. Department of Homeland Security has adopted the Common Vulnerability Scoring System (CVSS v3) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v3 produces a numerical score as well as a textual representation of that score reflecting the severity of a vulnerability. Scores range from 0.0 (no impact) to a maximum of 10.0 (critical impact with minimal effort to exploit). For additional information please refer to the CVSS v3.1 specifications.

Disclaimer

THE INFORMATION PROVIDED HEREIN IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND. AVEVA AND ITS AFFILIATES, PARENT AND SUBSIDIARIES DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY AVEVA, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES WILL CREATE A WARRANTY AND CUSTOMER MAY NOT RELY ON ANY SUCH INFORMATION OR ADVICE.
AVEVA DOES NOT WARRANT THAT THE SOFTWARE WILL MEET CUSTOMER'S REQUIREMENTS, THAT THE SOFTWARE WILL OPERATE IN COMBINATIONS OTHER THAN AS SPECIFIED IN AVEVA DOCUMENTATION OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.
IN NO EVENT WILL AVEVA OR ITS SUPPLIERS, DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY CUSTOMER OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF AVEVA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. AVEVA LIABILITY FOR DAMAGES AND EXPENSES HEREUNDER OR RELATING HERETO (WHETHER IN AN ACTION IN CONTRACT, TORT OR OTHERWISE) WILL IN NO EVENT EXCEED THE AMOUNT OF ONE HUNDRED DOLLARS ($100 USD).