DATE: 02/14/2022

SECURITY BULLETIN AVEVA-2021-007

Title

System Platform – Cleartext Credentials in Memory and Diagnostic Memory Dumps

Rating

High

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. ("AVEVA") has created security updates for supported versions to address vulnerabilities in AVEVA™ System Platform 2020 R2 P01 and all prior versions. The vulnerabilities could expose cleartext credentials for the Network User Account of the system, or cleartext credentials for the logged-in user, to an authorized, low privilege user. The cleartext credentials would also be exposed if the user creates a diagnostic memory dump of the relevant process and saves it to a non-protected location where an unauthorized, malicious user can access it.

Vulnerabilities have been addressed in:

- AVEVA™ Application Server
- AVEVA™ Operations Management Interface (OMI)
- AVEVA™ Historian and Historian Client

Recommendations

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

Customers using System Platform 2020 R2 P01 and all prior versions are affected and should upgrade to one of the versions listed below as soon as possible, then apply the corresponding security update:

Version	Security Update	Download Link
AVEVA™ System Platform 2020 R2 P01 AVEVA™ System Platform 2020 R2	AVEVA™ System Platform 2020 R2 SP1	**https://softwaresupportsp.aveva.com/#/producthub/details?id=c24f66e0-7e8f-4abb-0655-08d98ee90456**
AVEVA™ System Platform 2020	AVEVA™ System Platform 2020 P01	**https://softwaresupportsp.aveva.com/#/producthub/details?id=e6b5c987-b842-4c9f-406a-08d9be522504**

Vulnerability Characterization and CVSSv3 Rating

CWE-316: Cleartext Storage of Sensitive Information in Memory

8.1 | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:L

Acknowledgements

AVEVA would like to thank:

- **Sharon Brizinov of Claroty** for the independent discovery and responsible disclosure of these vulnerabilities
- **Ilya Karpov, Evgeniy Druzhinin and Konstantin Kondratev of Rostelecom-Solar** for the independent discovery and responsible disclosure of these vulnerabilities
- **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).