

SECURITY BULLETIN AVEVA-2021-001

Title

InTouch - Cleartext Password in WindowViewer Diagnostic Memory Dumps

Rating

Medium

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. (“AVEVA”) has created security updates for supported versions to address a vulnerability that exists in InTouch 2020 R2 and all prior versions. The vulnerability could expose clear-text credentials from InTouch Runtime (WindowViewer) if an authorized, privileged user creates a diagnostic memory dump of the process and saves it to a non-protected location where an unauthorized, malicious user can access it.

Recommendations

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

Customers using InTouch 2020 R2 and all prior versions are affected and should first upgrade to one of the versions listed below, then apply the corresponding security update:

Version	Security Update	Download Link
InTouch 2020 R2	InTouch 2020 R2 P01	https://softwaresupportsp.aveva.com/#/producthub/details?id=3ea6b4aa-9f1b-4741-7228-08d9066419ff
InTouch 2020	SecurityUpdate #1216934	https://softwaresupportsp.aveva.com/#/producthub/details?id=616677de-6c20-4a52-1a38-08d913b409f7
InTouch 2017 U3 SP1 P01	SecurityUpdate #1216933	https://softwaresupportsp.aveva.com/#/producthub/details?id=5ccf66c9-1424-4314-74aa-08d913b5544d

Vulnerability Characterization and CVSSv3 Rating

CWE-316: [Clear Text Storage of Sensitive Information in Memory](#)

InTouch Runtime (WindowViewer):

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

Acknowledgements

AVEVA would like to thank:

- **Ilya Karpov, Evgeniy Druzhininand, and Konstantin Kondratev of Rostelecom-Solar** for the discovery and responsible disclosure of this vulnerability
- **ICS-Cert and FSTEC** 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 specification](#).

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).