DATE: 06/25/2021

SECURITY BULLETIN AVEVA-2021-002

Title

System Platform - Vulnerabilities in AutoBuild Chaining to Arbitrary Code Execution or Denial of Service

Rating

High

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. ("AVEVA") has created a security update to address vulnerabilities in AutoBuild. **The vulnerable AutoBuild component is present in AVEVA™ System Platform versions 2017 through 2020 R2 P01 (inclusive)**. The vulnerabilities, if exploited and chained together, could allow a malicious entity to execute arbitrary code with system privileges or cause a denial of service.

Recommendations

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

The AutoBuild service is intended to be used only on the GR Node of System Platform during configuration. It should be disabled in all Runtime nodes using the Windows Service applet. Furthermore, if the AutoBuild functionality is not utilized on the GR Node, the AutoBuild service can also be disabled on the GR Node as an alternative mitigation that does not require patching.

Customers who need to continually use the AutoBuild functionality and cannot disable it in System Platform versions 2017 through 2020 R2 P01 (inclusive) are affected by the vulnerabilities and should first upgrade to one of the System Platform versions listed below, then apply the corresponding security update:

Version	Security Update	Download Link
System Platform 2020 R2 P01 2020 R2 2020	Apply AVEVA™ Communication Drivers Pack 2020 R2.1	https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=24f8a620-7b2e-4cd9-5973-08d91f9da2f8
System Platform 2017 U3 SP1 P01	First apply AVEVA™ Communication Drivers Pack 2020 R2* Then apply AVEVA™ Communication Drivers Pack 2020 R2.1	https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=ab14203d-b658-4ffa-fdb1-08d8b7ea05ec https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=24f8a620-7b2e-4cd9-5973-08d91f9da2f8

*Note: Activated Licensing is required to apply AVEVA™ Communication Drivers Pack 2020 R2 on top of System Platform 2017 U3 SP1 P01. For information on license compatibility, please contact Support.

Vulnerability Characterization and CVSS Rating

CWE-22: Path Traversal
CWE-306: Missing Authentication for Critical Function
CWE-346: Origin Validation Error
CWE-347: Improper Verification of Digital Signature
AutoBuild Code Execution Vulnerability Chain: **8.8** | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE-248: Uncaught Exception
AutoBuild Denial of Service: **6.5** | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Acknowledgements

AVEVA would like to thank:

- **Sharon Brizinov of Claroty** for the discovery, responsible disclosure of the vulnerabilities, and verifying AVEVA's fixes
- **ICS-Cert** for coordination of advisories and CVE creation

Support

For information on how to reach AVEVA Customer 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 AVEVA Customer 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).