DATE: 08/11/2021

SECURITY BULLETIN AVEVA-2021-003

Title

SuiteLink Server – Multiple Denial of Service (DoS) Vulnerabilities and theoretical Remote Code Execution (RCE)

Rating

High

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. (“AVEVA”) has created a security update to address vulnerabilities in the SuiteLink Server. The vulnerabilities, if exploited, will cause the SuiteLink Server to crash while parsing a malicious packet. Additionally, it may theoretically be possible to achieve Remote Code Execution, but no proof-of-concept exists. SuiteLink Clients are not affected by this vulnerability and do not need to be patched.

The following products ship a vulnerable version of the SuiteLink Server and are affected:

- AVEVA™ System Platform 2020 R2 P01 and all prior versions
- AVEVA™ InTouch 2020 R2 P01 and all prior versions
- AVEVA™ Historian 2020 R2 P01 and all prior versions
- AVEVA™ Communication Drivers Pack 2020 R2 and all prior versions
- AVEVA™ Operations Integration Core 3.0 and all prior versions
- AVEVA™ Data Acquisition Servers all versions
- AVEVA™ Batch Management 2020 and all prior versions
- AVEVA™ MES 2014 R2 and all prior versions

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 products should apply the corresponding security update. Note that a subset of the updates require Activation-based Licensing.

Version	Security Update	Download Link
AVEVA™ System Platform 2014 R2 SP1 P02 through 2020 R2 P01 (inclusive)	AVEVA™ SuiteLink 3.2.002	https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=74691731-8acb-4955-2d86-08d91f9dec02

Version	Security Update	Download Link
AVEVA™ InTouch 2014 R2 SP1 P02 through 2020 R2 P01 (inclusive)	AVEVA™ SuiteLink 3.2.002	https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=74691731-8acb-4955-2d86-08d91f9dec02
AVEVA™ Historian 2014 R2 SP1 P02 through 2020 R2 P01 (inclusive)	AVEVA™ SuiteLink 3.2.002	https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=74691731-8acb-4955-2d86-08d91f9dec02
AVEVA™ Communication Drivers Pack 2020 R2 and prior	AVEVA™ SuiteLink 3.2.002 Or AVEVA™ Communication Drivers Pack 2020 R2.1 (Note: Activation-based Licensing is required, please contact Support for information on license compatibility)	https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=74691731-8acb-4955-2d86-08d91f9dec02 https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=24f8a620-7b2e-4cd9-5973-08d91f9da2f8
AVEVA™ Operations Integration Core 3.0 and prior		
All mature versions of all Data Acquisition Servers		
AVEVA™ Batch Management 2020	AVEVA™ SuiteLink 3.2.002	https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=74691731-8acb-4955-2d86-08d91f9dec02
AVEVA™ Batch Management 2017 U1 and prior	First upgrade to AVEVA™ Batch Management 2020 Then apply AVEVA™ SuiteLink 3.2.002	https://softwaresupportsp.aveva.com/#/producthub/details?id=d65cd14a-f3b6-4340-a830-0df5f9c0da79 https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=74691731-8acb-4955-2d86-08d91f9dec02
AVEVA™ MES 2014 R2 and prior	Upgrade to AVEVA™ MES 2014 R3 or higher	https://softwaresupportsp.aveva.com/#/producthub/details?id=7c87fe29-f137-4f74-3197-08d86ac74c47

Vulnerability Characterization and CVSS v3 Rating

CWE-122: Heap-Based Buffer Overflow

SuiteLink Server (theoretical RCE):	**8.1** | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
SuiteLink Server DoS:	**7.5** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE-476: Null Pointer Dereference

SuiteLink Server DoS:	**7.5** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE-755: Improper Handling of Exceptional Conditions:

SuiteLink Server DoS:	**7.5** | CVSS:3.1/AV:N/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 Common Vulnerability and Exposure (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).