DATE: 11/14/2023

SECURITY BULLETIN AVEVA-2023-003

Title
AVEVA™ Operations Control Logger: Local Privilege Escalation and Arbitrary File Delete Vulnerabilities

Rating
High

Published By
AVEVA Product Security Response Center

Overview
AVEVA Group Limited on behalf of itself and its subsidiaries ("AVEVA") has created a security update to address vulnerabilities in the AVEVA Operations Control Logger (formerly known as ArchestrA Logger), impacting the following products:

- AVEVA System Platform 2020 R2 SP1 P01 and all prior versions
- AVEVA Historian 2020 R2 SP1 P01 and all prior versions
- AVEVA Application Server 2020 R2 SP1 P01 and all prior versions
- AVEVA InTouch 2020 R2 SP1 P01 and all prior versions
- AVEVA Enterprise Licensing 3.7.002 and all prior versions (formerly known as License Manager)
- AVEVA Manufacturing Execution System 2020 P01 and all prior versions (formerly known as Wonderware MES)
- AVEVA Recipe Management 2020 Update 1 Patch 2 and all prior versions
- AVEVA Batch Management 2020 SP1 and all prior versions
- AVEVA Edge 2020 R2 SP1 P01 and all prior versions (formerly known as Indusoft Web Studio)
- AVEVA Work Tasks 2020 U2 and all prior versions (formerly known as Workflow Management)
- AVEVA Plant SCADA 2020 R2 Update 15 and all prior versions (formerly known as Citect)
- AVEVA Mobile Operator 2020 R1 and all prior versions (formerly known as IntelaTrac Mobile Operator Rounds)
- AVEVA Communication Drivers Pack 2020 R2 SP1 and all prior versions
- AVEVA Telemetry Server 2020 R2 SP1 and all prior versions

Vulnerability Technical Details

1. Local Privilege Escalation

The vulnerability, if exploited, could allow a local OS-authenticated user with standard privileges to escalate to System privilege on the machine where these products are installed, resulting in complete compromise of the target machine.

CWE-250: Execution with Unnecessary Privileges
CVSSv3.1: **7.8 High** | AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2023-33873

2. Local Arbitrary File Delete

The vulnerability, if exploited, could allow a local OS-authenticated user with standard privileges to delete files with System privilege on the machine where these products are installed, resulting in Denial of Service.

CWE-73: External Control of File Name or Path
CVSS v3.1: **5.5 Med** | AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CVE-2023-34982

Recommendations

AVEVA recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation. Customers using affected products should apply security updates as soon as possible.

In addition to applying the security updates, customers should take the following general precautions:

- Ensure that Guest or Anonymous local OS accounts are disabled.
- Ensure that only trusted users are able to login on the nodes where their Operations Control Logger is running.

Security Updates

Known Compatibility Issues:
AVEVA System Platform 2020 through 2020 R2 SP1 cannot be newly installed on top of other AVEVA products which have been previously patched with the Operations Control Logger v22.1. For additional details please refer to Alert 000038736.

AVEVA System Platform, Historian, Application Server, and InTouch 2020 through 2020 R2 SP1 P01 (inclusive):

- Recommended fix: upgrade to AVEVA System Platform 2023 or higher.
  https://softwaresupportsp.aveva.com/#/producthub/details?id=64d4e12b-c363-4f35-8e8e-08da716924f7
- Alternative fix: Install AVEVA Operations Control Logger v22.1 or higher.
  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

AVEVA System Platform, Historian, Application Server, and InTouch versions 2017 U3 SP1 P01 and all prior:

- Recommended fix: upgrade to AVEVA System Platform 2023 or higher.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=64d4e12b-c363-4f35-8e8e-08da716924f7

- Alternative fix: First upgrade to AVEVA System Platform 2020 R2 SP1, then install Operations Control Logger v22.1 or higher. Please review Known Compatibility Issues

  https://softwaresupportsp.aveva.com/#/producthub/details?id=c24f66e0-7e8f-4abb-0655-08d98ee90456
  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

AVEVA Enterprise Licensing 3.7.002 and all prior versions:

- Recommended fix: upgrade to AVEVA Enterprise Licensing 4.0 or higher.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=23f2f464-b581-4890-9b7e-079d38f9a7dd

- Alternative fix: Install AVEVA Operations Control Logger v22.1 or higher. Please review Known Compatibility Issues

  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

AVEVA Manufacturing Execution System 2020 P02 and all prior versions:

- Recommended fix: upgrade to AVEVA MES 2023 or higher.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=50f245ed-210d-4047-8153-08daf99ef086

- Alternative fix: Install AVEVA Operations Control Logger v22.1 or higher. Please review Known Compatibility Issues.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

AVEVA Recipe Management 2020 Update 1 Patch 2 and all prior versions:

- Recommended fix: upgrade to AVEVA Recipe Management 2023 or higher.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=6e32c383-6be1-43d6-2a52-08db0eab7760

- Alternative fix: Install AVEVA Operations Control Logger v22.1 or higher. Please review Known Compatibility Issues.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

AVEVA Batch Management 2020 SP1 and all prior versions:

- Recommended fix: upgrade to AVEVA Batch Management 2023 or higher.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=b7fff900-39af-4d54-b8e7-210fd2d96a57

- Alternative fix: Install AVEVA Operations Control Logger v22.1 or higher. Please review Known Compatibility Issues.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

AVEVA Edge 2020 R2 SP1 P01 and all prior versions (formerly known as Indusoft Web Studio)

- Recommended fix: upgrade to AVEVA Edge 2023 or higher.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=0c8abaf3-2e4c-4be1-aa78-3ad445c58a16

- Alternative fix 1: Install AVEVA Edge 2020 R2 SP2 or higher.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=bd805851-0c68-4343-15ee-08da9a4aa617

- Alternative fix 2: Install AVEVA Operations Control Logger v22.1 or higher. Please review Known Compatibility Issues.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

AVEVA Work Tasks 2020 U2 and all prior versions (formerly known as Workflow Management)

- Recommended fix: upgrade to AVEVA Work Tasks 2023 SP1 or higher. If AVEVA Work Tasks is used together with System Platform, both products will need to be upgraded to a compatible version. Please review the Technology Matrix.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=74b0e8a6-80c2-4884-a689-08daefd8f20e

- Alternative fix: Install AVEVA Operations Control Logger v22.1 or higher. Please review Known Compatibility Issues.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

AVEVA Plant SCADA 2020 R2 Update 15 (May ’23) and all prior versions (formerly known as Citect)

- Recommended fix: upgrade to AVEVA Plant SCADA 2023 or higher.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=892087d6-af69-439f-70f1-08da91049ae3

- Alternative fix 1: Install Plant SCADA 2020 R2 Update 16 (Jun ’23) or higher.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=78809d30-3f97-45c3-8d71-f537909aa3b5

- Alternative fix 2: Install AVEVA Operations Control Logger v22.1 or higher. Please review Known Compatibility Issues.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

AVEVA Mobile Operator 2020 R1 and all prior versions (formerly IntelaTrac Mobile Operator)

- Recommended fix: upgrade to AVEVA Mobile Operator 2020 R2 or higher.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=da960462-b522-4031-f287-08db1b42b39a

- Alternative fix 1: For Mobile Operator 2020 through 2020 R1, install AVEVA Operations Control Logger v22.1 or higher. Please review Known Compatibility Issues.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

- Alternative fix 2: For IntelaTrac Mobile Operator 2017 SP2 and prior, first upgrade to AVEVA Mobile Operator 2020, then install AVEVA Operations Control Logger v22.1 or higher. Please review Known Compatibility Issues.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=37a51ba1-4a40-4c69-44cd-08d8fd519f4f
  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

AVEVA Communication Drivers Pack 2020 R2 SP1 and all prior versions

- Recommended fix: upgrade to AVEVA Communication Drivers Pack 2023.1 or higher.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=e1af0884-b3c6-4d0f-a6b6-47507b398690

- Alternative fix: Install AVEVA Operations Control Logger v22.1 or higher. Please review Known Compatibility Issues.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

AVEVA Telemetry Server 2020 R2 SP1 and all prior versions

- Recommended fix: upgrade to AVEVA Telemetry Server 2020 R2 SP2 or higher.

  https://softwaresupportsp.aveva.com/#/connectivityhub/details?id=4bbbab19-b1b2-4b0d-ba12-08dafa4ad12d

- Alternative fix: Install AVEVA Operations Control Logger v22.1 or higher. Please review Known Compatibility Issues.

  https://softwaresupportsp.aveva.com/#/producthub/details?id=11aef286-169f-4a12-5e32-08db1b4400c8

Acknowledgements

AVEVA would like to thank:

- **Lukasz Piotrowski** from **Equinor** for the discovery, responsible disclosure, and testing fixes
- **CISA** 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 v3.1)

The U.S. Department of Homeland Security has adopted the Common Vulnerability Scoring System (CVSS v3.1) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v3.1 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.

Coordination with Authorities

Organizations observing suspected malicious activity should follow established internal procedures and report findings to applicable authorities for tracking and correlation against other incidents.

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).