

SECURITY BULLETIN AVEVA-2020-001

Title

SQL Injection in AVEVA™ Enterprise Data Management Web (formerly eDNA Web)

Rating

High

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. (“AVEVA”) has created a security update to address SQL Injection vulnerabilities in AVEVA™ Enterprise Data Management Web v2019 and all prior versions formerly known as eDNA Web.

The vulnerabilities exist in a component of eDNA Web and, if exploited, could allow a malicious entity to execute arbitrary SQL commands under the privileges of the account configured in eDNA Web for SQL access. If eDNA Web is not installed, then the deployment is not vulnerable to SQL Injections and no further action is necessary.

Recommendations

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

Customers using affected versions are recommended to upgrade to AVEVA™ Enterprise Data Management Web v2019 SP1 as soon as possible. If an upgrade to v2019 SP1 is not possible, upon request to AVEVA Global Customer Support, a hotfix can be made available for eDNA Web v2018 SP2. Other versions will not be hot-fixed and must be upgraded. For help with applying upgrades and hot fixes, please contact AVEVA Global Customer Support.

Security Update

The following Security Update addresses the vulnerabilities outlined in this Security Bulletin:

Sept 09, 2020: AVEVA™ Enterprise Data Management Web v2019 SP1

<https://softwaresupportsp.aveva.com/#/producthub/details?id=53497>

Vulnerability Characterization and CVSSv3 Rating

CWE-089: Improper Neutralization of special elements in SQL Command/Query

v2017-v2019

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

versions prior to v2017

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

Acknowledgements

AVEVA would like to thank:

- **Yuri Kramarz of Cisco Talos** for the discovery, responsible disclosure of the vulnerabilities, and retesting fixes in AVEVA™ Enterprise Data Management Web v2019 SP1.
 - **ICS-Cert and Cisco Talos** for coordination of advisories and CVEs
-

Support

For information on how to reach AVEVA support for your product, please refer to this link: [AVEVA Software Global 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 [CVSSv3 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).