Date: 01/24/2019

AVEVA Security Bulletin LFSEC00000135

Title

Wonderware System Platform Vulnerability – Potential for Unauthorized Access to Credentials

Rating

High

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. (“AVEVA”) has released a new version of System Platform which includes a security update to address vulnerabilities in **Wonderware System Platform 2017 Update 2 and all prior versions**.

These vulnerabilities could allow unauthorized access to the credentials for the ArchestrA Network User Account.

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

Recommendations

Customers using **Wonderware System Platform 2017 Update 2 and all prior versions** are affected and should upgrade to **System Platform 2017 Update 3** as soon as possible.

For information regarding how to secure Industrial Control Systems please reference NIST SP800-82r2.

Vulnerability Details

System Platform utilizes an ArchestrA Network User Account for authentication of system processes and inter-node communications. An unauthorized user could make use of an API to obtain the credentials for this account.

Security Update

The following Security Updates address the vulnerabilities outlined in this Security Bulletin: **System Platform 2017 Update 3.**

Affected Products, Components, and Corrective Security Update

The following table identifies the currently supported products affected. Software updates can be downloaded from the Global Customer Support "Software Download" area or from the links below:

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Security Update
Wonderware System Platform 2017 Update 2 and all prior versions	Multiple	Confidentiality, Integrity, Availability	High	https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=52332

Vulnerability Characterization and CVSSv3 Rating

CWE-522: Insufficiently Protected Credentials, CWE-250: Execution with Unnecessary Privileges, CWE-862: Missing Authorization

- Wonderware System Platform 2017 Update 2 and all prior versions:
  8.8 | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Acknowledgements

AVEVA would like to thank:

- **Vladimir Dashchennko from Kaspersky Lab** for the discovery and responsible disclosure of this vulnerability
- **ICS-Cert** for coordination of advisories

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