Date: 07/13/2018

AVEVA Security Bulletin LFSEC00000127

Title

InTouch Remote Code Execution on locales that do not use a dot floating point separator

Rating

Critical

Published By

AVEVA Software Security Response Center

Overview

AVEVA Software, LLC. (“AVEVA”) has created a security update to address vulnerabilities in:

- **InTouch 2017 Update 2**
- **InTouch 2014 R2 SP1**

The vulnerabilities, if exploited on operating system locales that do not use a dot floating point separator, could allow an unauthenticated user to remotely execute code with the same privileges as those of the InTouch View process.

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

Recommendations

Customers using **InTouch 2017 Update 2** are affected and should apply **HF-17_2/CR149706** as soon as possible. Customers using **InTouch 2017 or 2017 Update 1** are also affected and should first upgrade to InTouch 2017 Update 2, then apply **HF-17_2/CR149706.**

Customers using **InTouch 2014 R2 SP1** are affected and should apply **HF-11_1_SP1/CR149705** as soon as possible. Customers using versions of **InTouch older than 2014 R2 SP1** are also affected and should first upgrade to a supported version of InTouch and then apply the corresponding hotfix.

Vulnerability Details

InTouch provides the capability for an HMI client to read and write tags defined in a view. A remote unauthenticated user could send a carefully crafted packet to exploit a stack-based buffer overflow vulnerability with potential for code to be executed while performing a tag-write operation on a locale that does not use a dot floating point separator. The code would be executed under the privileges of the InTouch View process and could lead to a compromise of the InTouch HMI.

Security Update

The following Security Updates address the vulnerabilities outlined in this Security Bulletin:
July 13, 2018: InTouch 2017 Update 2 HF-17_2/CR149706
July 13, 2018: InTouch 2014 R2 SP1 HF-11_1_SP1/CR149705

Affected Products, Components, and Corrective Security Patches

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
InTouch 2017 Update 2	Multiple	Confidentiality, Integrity, Availability	Critical	https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=5058
InTouch 2014 R2 SP1	Multiple	Confidentiality, Integrity, Availability	Critical	https://softwaresupportsp.schneider-electric.com/#/producthub/details?id=5057

Vulnerability Characterization and CVSSv3 Rating

CWE-121: Stack-based Buffer Overflow

- InTouch running on a locale that does not use a dot floating point separator
  9.8 | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Acknowledgements

AVEVA would like to thank:
- **George Lashenko from CyberX** 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

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’S 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’S 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).