PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2021/32

AVEVA System Platform using AVEVA Application Server, AVEVA Operations Management Interface, and AVEVA Historian (server & client) modules

Version 2020 R2

Paris, le 27 janvier 2022

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CSPN-2021/32

Nom du produit

AVEVA System Platform using AVEVA Application Server, AVEVA Operations Management Interface, and AVEVA Historian (server & client) modules

Référence/version du produit

Version 2020 R2

Catégorie de produit

Autre : SCADA

Critère d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

AVEVA SA
5 Square Félix Nadar
94300 Vincennes

Développeur

AVEVA Solutions Ltd
High Cross Madingley Road
Cambridge,
Royaume Uni

Centre d'évaluation

OPPIDA
6 avenue du vieil étang
78180 Montigny le Bretonneux

Fonctions de sécurité évaluées

Protection contre les entrées malformées
Communications sécurisées
Connection sécurisée avec le serveur d'authentification
Stockage sécurisé des secrets
Contrôle d'accès
Intégrité et confidentialité de la configuration

Fonctions de sécurité non évaluées

Sans objet

Restriction(s) d'usage

Oui (cf. §3.2)

PREFACE

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est «AVEVA System Platform using AVEVA Application Server, AVEVA Operations Management Interface, and AVEVA Historian (server & client) modules, Version 2020 R2» développé par AVEVA SA.

AVEVA System Platform permet de développer des interfaces homme-machine (IHM) et de les déployer dans le contexte d'un système SCADA. Il comporte trois composants :

- *Application Object Server (ou Application Server)*, qui permet d'exécuter le code ;
- *Historian* qui fournit les données d'historisation, les alarmes et les évènements destinés à l'*Application Server* ;
- les *drivers* qui permettent la communication avec les contrôleurs tierce partie, comme des automates programmables ou des RTU (*Remote Terminal Unit*).

La TOE inclut, en plus d'*AVEVA System Platform,* deux applications servant de clients :

- un *Supervisory client* permettant d'exécuter l'interface opérateur (visualisation des synoptiques et *process*), et consultation en temps réel des données, alarmes et évènements remontées par l'*Application Server*. Le client choisi pour cette évaluation est *AVEVA Operations Management Interface* (ou AVEVA OMI) ;
- un *Historian Client*, permettant d'accéder et de visualiser les données agrégées par le composant *Historian*, sous la forme de tableaux ou de courbes.

La figure ci-dessous explicite l'architecture fonctionnelle du produit.

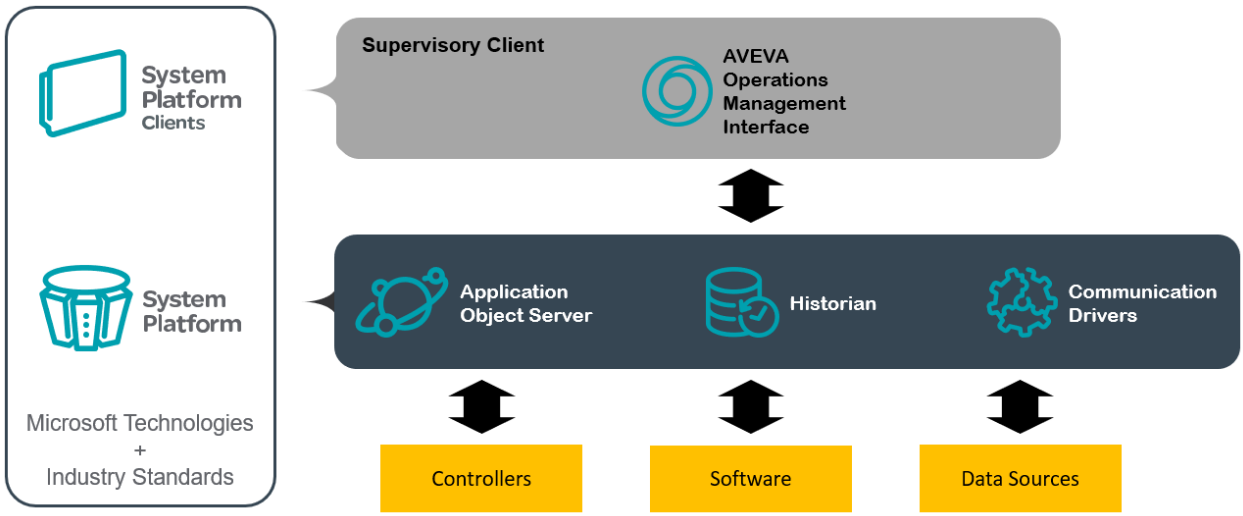

Figure 1 - Architecture Produit.

1.2 Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1 *Catégorie du produit*

☐	1	détection d'intrusions
☐	2	anti-virus, protection contre les codes malicieux
☐	3	pare-feu
☐	4	effacement de données
☐	5	administration et supervision de la sécurité
☐	6	identification, authentification et contrôle d'accès
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☐	9	stockage sécurisé
☐	10	environnement d'exécution sécurisé
☐	11	terminal de réception numérique (*Set top box*, STB)
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☒	**99**	**Autre : SCADA**

1.2.2 *Identification du produit*

Produit	
Nom du produit	AVEVA System Platform using AVEVA Application Server, AVEVA Operations Management Interface, and AVEVA Historian (server & client) modules
Numéro de la version évaluée	Version 2020 R2

La version certifiée du produit est l'agrégation de plusieurs composants, chacun étant identifié séparément. Afin de vérifier qu'il dispose bien des versions évaluées, l'utilisateur doit consulter le fichier *readme* fourni dans l'ISO d'installation livré par AVEVA :

Included in This Release

Program Name	Version
AVEVA Application Server 2020 R2 including AVEVA OMI	20.1.000
AVEVA Communication Drivers Pack 2020 R2	7.2.0
AVEVA Enterprise License Manager	3.7.00000
AVEVA Enterprise License Server	3.7.00000
AVEVA Enterprise Licensing Platform	3.7.00000
AVEVA Historian, formerly Wonderware 2020 R2	20.1.000
AVEVA Historian Client 2020 R2	20.1.000
AVEVA InTouch HMI, formerly Wonderware 2020 R2	20.1.000
AVEVA InTouch Access Anywhere Server 2020 R2	20.1.000
AVEVA InTouch Access Anywhere Secure Gateway 2020 R2	20.1.000
Insight Publisher	4.2.000
Platform Common Services 4.5.1	4.5.20340.1
System Monitor Agent Install Manager 1.3	1.3.0
System Monitor Manager 1.3	1.3.0

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la protection contre les entrées malformées ;
- les communications sécurisées ;
- la connexion sécurisée avec le serveur d'authentification ;
- le stockage sécurisé des secrets ;
- le contrôle d'accès ;
- l'intégrité et la confidentialité de la configuration.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond à un déploiement en machines virtuelles. La plateforme de test est constituée des éléments suivants :

- Machine 1 : *Galaxy Repository* (GR), *Historian* (HIST) et serveur de licence (LS) ;
- Machine 2 : *Application Object Server* (AOS) et *Data Acquisition Server* (DAS) ;
- Machine 3 : *Supervisory Clients* (OMI) ;
- Machine 4 : station d'ingénierie (IDE) et *System Management Server* (SMS) ;
- Machine 5 : simulation d'un automate et serveur OPC UA ;
- Machine 6 : *Active Directory*.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

2.2 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.2.1.2 Description de l'installation et des non-conformités éventuelles

L'installation a suivi la documentation fournie par AVEVA ; elle a été réalisée avec l'aide d'AVEVA.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source d'une partie de l'implémentation des mécanismes cryptographiques du produit, le reste de l'implémentation étant fourni par du code en source fermée (*.NET*).

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

2.2.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.2.7.2 Avis d'expert sur la facilité d'emploi

Sans objet.

2.2.7.3 Notes et remarques diverses

Sans objet.

2.3 Analyse de la résistance des mécanismes cryptographiques

Certains mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse n'a pas identifié de vulnérabilité exploitable pour le niveau d'attaquant visé.

Les mécanismes cryptographiques liés au canal TLS, à la signature, à la protection des mots de passe sont fournis par le système d'exploitation sous-jacent, en source fermée (voir section *security functions* de [CDS]). Il n'est donc pas possible d'en faire une analyse complète au sens de la méthodologie CSPN.

2.4 Analyse du générateur d'aléa

La TOE utilise le générateur d'aléa du système d'exploitation sous-jacent, en source fermée (voir section *security functions* de [CDS]). Il n'est donc pas possible d'en faire une analyse complète au sens de la méthodologie CSPN.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « AVEVA System Platform using AVEVA Application Server, AVEVA Operations Management Interface, and AVEVA Historian (server & client) modules, Version 2020 R2 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2 Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et suivre les recommandations détaillées dans les guides fournis [GUIDES], notamment :

- tenir le système d'exploitation sous-jacent à jour des derniers correctifs de sécurité ;
- désactiver TLS 1.0 et 1.1, et n'autoriser que l'utilisation de TLS 1.2 ;
- utiliser des mots de passe d'entropie équivalente à 80 bits ou plus, ce qui implique que :
    - Les mots de passe doivent être générés aléatoirement (par exemple en utilisant un gestionnaire de mots de passe) et non choisis par les utilisateurs ;
    - De plus, les mots de passe doivent être d'une complexité suffisante pour atteindre les 80 bits d'entropie. Par exemple :
        - 16 caractères dans un alphabet de 36 symboles (https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/); ou
        - 13 caractères ASCII imprimables,(https://en.wikipedia.org/wiki/Password_strength); ou encore
        - sept mots choisis selon la technique du *diceware* (https://en.wikipedia.org/wiki/Password_strength).

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : *AVEVA System Platform / AVEVA Operations Management Interface (OMI) / AVEVA Historian CSPN Security Target*, référence RnD CS 2020-0601, version 1.4, 1er décembre 2021.
[RTE]	Rapport technique d'évaluation : *CSPN Evaluation Technical Report – AVEVA HMI – AVEVA System Platform*, référence OPPIDA/CESTI/AVEVA HMI/RTE, version 1.4, 7 janvier 2022.
[GUIDES]	Guide d'installation/utilisation du produit : *Cyber Security Best Practices for System Platform, OMI, Historian 2020 R2 Installation and Operations*, référence TN000032836, 17 décembre 2021, accessible en ligne à l'adresse https://softwaresupportsp.aveva.com/#/okmimarticle/docid/tn000032836.

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 3.0, 12 avril 2021. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0,6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.