Reference: 2018-11-INF-2694-v1
Target: Público
Date: 07.02.2019

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2018-11**
TOE	**SolarWinds Orion Suite for Federal Government v3.0**
Applicant	**26-3798676 - SolarWinds Worldwide, LLC.**
References	

[EXT-3888] Certification request

[EXT-4545] Evaluation Technical Report

Certification report of the product SolarWinds Orion Suite for Federal Government v3.0, as requested in [EXT-3888] dated 05/04/2018, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-4545] received on 18/12/2018.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product SolarWinds Orion Suite for Federal Government v3.0.

The SolarWinds Orion 3.0 suite is a set of software applications and services executing on one or more Windows servers. The applications monitor a configured set of network-attached devices and applications for status, performance and configuration settings. Depending on the size of the network, multiple instances of the applications may be deployed on different servers to provide adequate performance. For enhanced availability and robustness, a failover configuration may be deployed.

Developer/manufacturer: SolarWinds Worldwide, LLC.

Sponsor: SolarWinds Worldwide, LLC..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Applus Laboratories.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 – EAL2 + ALC_FLR.2.

Evaluation end date: 24/07/2018.

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.2) have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2+ALC_FLR.2, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product SolarWinds Orion Suite for Federal Government v3.0, a positive resolution is proposed.

TOE SUMMARY

The Orion 3.0 software suite acts as a monitoring and management tool for use by network managers. It maintains a list of the managed elements in the network, monitors their operation, and alerts the network managers to specified conditions. Managed elements are network devices (e.g. routers and switches), servers, storage devices or applications that can be monitored by standard mechanisms such as SNMP, ICMP, Syslog or WMI. NCM functionality may be used to track configuration changes on the network devices for products that are able to download a copy of their current configuration parameters.

Users interact with the TOE via multiple mechanisms. The EOC Web Console and Orion Web Console are provided for remote interaction with the EOC and Orion functionality.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 and the evidences required by the additional component ALC_FLR.2, according to Common Criteria v3.1 R5.

ASE: Security Target Evaluation	ASE_INT.1. ST Introduction
	ASE.CCL.1. Conformance claims
	ASE_SPD.1. Security problem definition
	ASE_OBJ.2. Security objectives
	ASE_ECD.1. Extended component definition
	ASE_REQ.2. Derived security requirements
	ASE_TSS.1. TOE summary specification
ADV: Development	ADV_ARC.1. Security architecture
	ADV_FSP.2. Functional specification
	ADV_TDS.1. TOE design
AGC: Guidance documents	AGD_OPE.1. Operational user guidance
	AGD_PRE.1. Preparative procedures
ALC: Life cycle support	ALC_CMC.2. CM capabilities
	ALC_CMS.2. CM Scope
	ALC_DEL.1. Delivery
	ALC_FLR.2. Flaw remediation
ATE: Tests	ATE_COV.1. Coverage
	ATE_FUN.1. Functional tests
	ATE_IND.2. Independent testing
AVA: Vulnerability assessment	AVA_VAN.2. Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

FAU: Security audit	FAU_GEN.1. Security audit data generation
	FAU_SAR.1. Security audit review
	FAU_SAR.2. Security audit review
FIA: Identification and authentication	FIA_ATD.1. User attribute definition
	FIA_UAU.2. User authentication
	FIA_UAU.7. User authentication
	FIA_UID.2. User identification
	FIA_USB.1. User-subject binding
FMT: Security management	FMT_MTD.1. Management of TSF data
	FMT_SMF.1. Specification of management functions
	FMT_SMR.1. Security management roles
FNM: Network management	FNM_MDC.1. Monitor Data Collection
	FNM_ANL.1. Monitor Analysis
	FNM_RCT.1. Management React
	FNM_RDR.1. Restricted Data Review
	FNM_STG.1. Guarantee of Monitor Data Availability
FTA: TOE access	FTA_SSL.3. Session locking and termination

IDENTIFICATION

Product: SolarWinds Orion Suite for Federal Government v3.0

Security Target: SolarWinds Orion Software Security Target, version 1.12, July 16, 2018.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 - EAL2+ALC_FLR.2.

SECURITY POLICIES

The use of the product SolarWinds Orion Suite for Federal Government v3.0 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in [ST], chapter 3.4 (Organizational Security Policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.2 (Assumptions), are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST], chapter 3.3 (Threats) do not suppose a risk for the product SolarWinds Orion Suite for Federal Government v3.0, although the agents implementing attacks have the attack potential according to the Basic attack potential of EAL2+ALC_FLR.2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are detailed in [ST], chapter 4.2 (Security objectives for the operational environment).

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

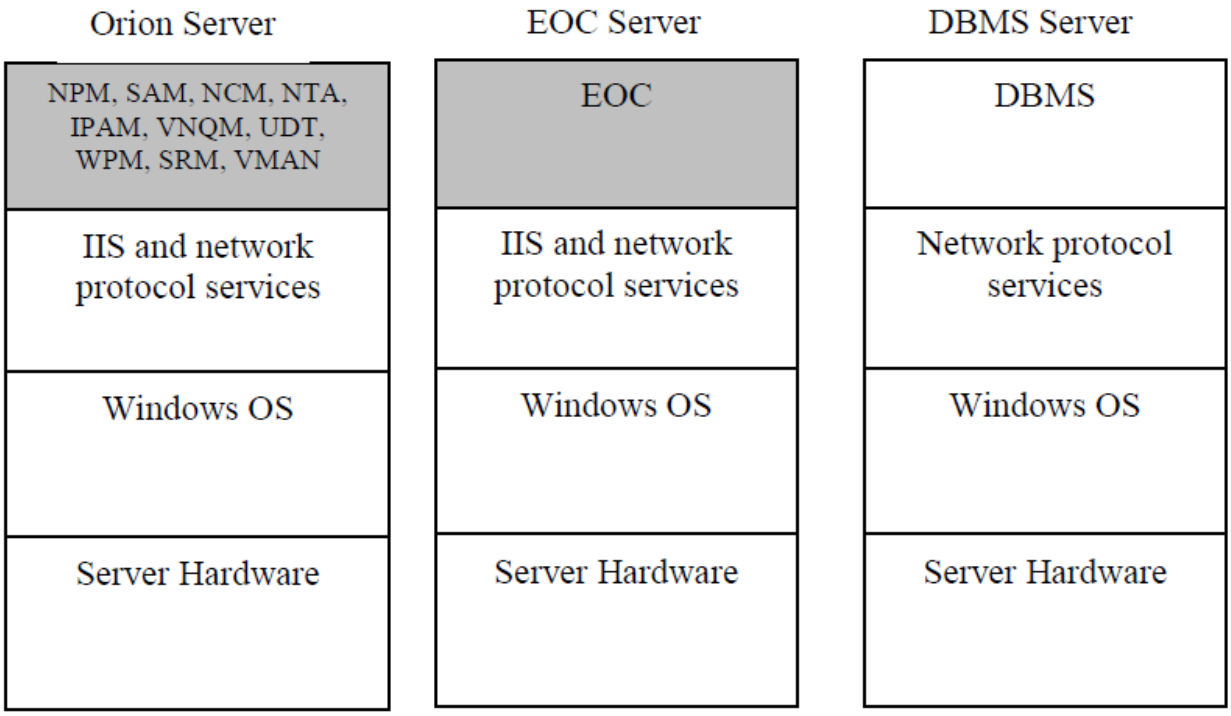
LOGICAL ARCHITECTURE

The TOE subsystems fall into one of two categories:

1. Orion monitoring and management subsystems (consisting of the subsystems associated with NPM, SAM, NCM, NTA, IPAM, VNQM, UDT, SRM, VMAN, and WPM).
2. EOC subsystem for aggregation of information from multiple Orion Servers.

PHYSICAL ARCHITECTURE

The TOE consists of the SolarWinds Orion 3.0 software identified in the previous section executing on multiple dedicated Windows servers. The physical architecture of the TOE is depicted in the figure below, with TOE components shaded. The operating systems (including the network protocol stacks and cryptographic functionality), web servers and DBMS are outside the TOE boundary.



DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

1. SolarWinds® Enterprise Operations Console Getting Started Version 2.0 (EOCv20AdministratorGuide.pdf)
2. SolarWinds® Network Performance Monitor Administrator Guide Version 12.2 (NPMv122AdministratorGuide.pdf)
3. SolarWinds® Server & Application Monitor Administrator Guide Version 6.6 (SAMv66AdministratorGuide.pdf)
4. SolarWinds® Network Configuration Manager Administrator Guide Version 7.7 (NCMv77AdministratorGuide.pdf)
5. SolarWinds® IP Address Manager Administrator Guide Version 4.6 (IPAMv46AdministratorGuide.pdf)
6. SolarWinds® NetFlow Traffic Analyzer Administrator Guide Version 4.2.3 (NTAv423AdministrationGuide.pdf)
7. SolarWinds® User Device Tracker Administrator Guide Version 3.3 (UDTv33AdministratorGuide.pdf)
8. SolarWinds® VoIP and Network Quality Manager Administrator Guide Version 4.4 (VNQMv44AdministratorGuide.pdf)
9. SolarWinds® Web Performance Monitor Administrator Guide Version 2.2 (WPMv22AdministratorGuide.pdf)
10. SolarWinds Storage Resource Monitor Administrator Guide Version 6.6 (SRMv66AdministratorGuide.pdf)
11. SolarWinds® Virtualization Manager Administrator Guide Version 8.2 (VMANv82AdministratorGuide.pdf)
12. SolarWinds® Orion® Suite for Federal Government Version 3.0 Common Criteria Supplement (OrionCommonCriteriaSupplement.pdf)
13. SolarWinds® Server & Application Monitor Getting Started Guide Version 6.6 (SAMv66GettingStartedGuide.pdf)

All guidance documentation is distributed as PDF files available from links on the SolarWinds Common Criteria Webpage.

PRODUCT TESTING

The developer established a testing approach in order to test the main functionalities of the most important subsystems and security mechanisms of TOE. In doing so, the test performed covered all TSFIs but three (Netflow, WPM Recorder and Main) and all the SFRs except for FTA_SSL.3. However,

these TSFIs and SFR have been tested as part of the independent testing plan done by the evaluator.

All the tests have been performed by the developer in its premises, with a satisfactory result. During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the Security Target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

The evaluator has devised the testing plan by considering the following factors:

- SFRs.
- TSFIs.
- Subsystems.
- Especially complex or critical interfaces.
- Interfaces on which there are doubts about its operation.
- Developer testing effort.

It has been checked that the obtained results conform to the expected results.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product SolarWinds Orion Suite for Federal Government v3.0 it is necessary the disposition of the following software components:

- SolarWinds Orion Platform V2017.3.5 SP5
- Network Performance Monitor (NPM) V12.2
- Network Configuration Manager (NCM) V7.7
- Server & Application Monitor (SAM) V6.6
- Netflow Traffic Analyzer (NTA) V4.2.3
- IP Address Manager (IPAM) V4.6
- VoIP & Network Quality Manager (VNQM) V4.4.1
- User Device Tracker (UDT) V3.3
- Web Performance Monitor (WPM) V2.2.1
- Storage Resource Monitor (SRM) V6.6
- Virtualization Manager (VMAN) V8.2

- Enterprise Operations Console (EOC) V2.0.

Regarding the non-TOE hardware components, the only requirement is that they shall support the software elements previously detailed.

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the evaluation consists in three separated servers:

1. EOC Server: EOC installed on a dedicated server includes the Orion Enterprise Operations Console (EOC) V2.0.
2. Orion Server: Orion installed on a dedicated server with all the components included within the scope of the evaluation (except for EOC): Network Performance Monitor (NPM) V12.2, Network Configuration Manager (NCM) V7.7, Server & Application Monitor (SAM) V6.6, Netflow Traffic Analyzer (NTA) V4.2.3, IP Address Manager (IPAM) V4.6, VoIP & Network Quality Manager (VNQM) V4.4.1, User Device Tracker (UDT) V3.3, Web Performance Monitor (WPM) V2.2.1, Storage Resource Monitor (SRM) V6.6 and Virtualization Manager (VMAN) V8.2.
3. DB Server: Database and DBMS installed in a separate dedicated Windows server.

The following installation and configuration options must be used:

1. IIS on all the dedicated Windows servers hosting TOE components is configured to accept HTTPS connections only.
2. The SolarWinds Toolset optional component is not installed.
3. Session timeouts are not disabled for user accounts, and the Session Timeout for web users is configured as a non-zero value.
4. Windows Account Login is not enabled for the Orion Web Console.
5. Enable Audit Trails is selected.
6. Access to the Windows applications to invoke the TOE is restricted in Windows to users authorized to perform those functions, in particular: backup and restore the database, manage TOE Alerts, and manage Report configuration settings.
7. The Customize option is not configured for any menu bars for the Orion Web Console.
8. External web sites are not added to Orion Web Console views.
9. The “Check for product updates” function is disabled. Installing updates may update the component to a version that has not been evaluated.
10. Custom device pollers are not configured or evaluated. Pollers supplied with the TOE are included in the evaluation.
11. Custom component monitors are not configured or evaluated. Component monitors supplied with the TOE are included in the evaluation.

12. Custom property functionality is not configured or evaluated. Built-in properties are included in the evaluation and may be used to configure View limitations.
13. Advanced Alerts are not configured or evaluated. Basic Alerts are included in the evaluation.
14. Customized Views are not configured on the Orion Web Console.
15. View Limitations are not configured.
16. Custom account limitations are not configured.
17. The functionality to remotely manage interfaces in Network Devices is not evaluated.
18. Custom IPAM roles are not defined; the built-in IPAM roles are used exclusively.
19. Properties of IPAM-specific entities are not used to delegate access.
20. The SAM and WPM components allow for separately-configurable roles. The evaluated configuration requires the SAM and WPM component-specific roles to be configured the same as the Orion role (Administrator or User).
21. The NTA Database Maintenance option is enabled in order to have the TOE automatically compress and purge data according to the configured periods.
22. When importing User Accounts into the TOE, only individual accounts are imported. Windows Group Accounts are not imported.
23. Only Administrators assign passwords for User Accounts defined in the TOE. Non-Administrators are not permitted to change their own passwords.
24. The Orion Server Browser Integration parameter is not enabled for User Accounts, since the operations performed via this integration are outside the control of the TOE.
25. Reports are managed via the Orion Web Console rather than the Report Writer Windows application (legacy).
26. Custom NCM device templates are not configured or evaluated. The default device templates supplied with the TOE are included in the evaluation.
27. Custom Configuration Change Templates are not configured or evaluated. The default configuration change templates supplied with the TOE are included in the evaluation.
28. Real-time config change notification is not enabled in NCM since it is dependent on additional software beyond the scope of the evaluated components.
29. Per-device credentials are used rather than per-user device credentials.
30. The Allow User To Personalize Their Pages permission is not set for any EOC user accounts. Therefore, only the default page views are included in the evaluation.
31. If TFTP is used to exchange configuration files with Nodes, the TFTP service is restricted to requests from authorized Nodes.

32. The SolarWinds Cortex service is disabled on all of the dedicated Windows servers hosting TOE components so that the REST interface is not available.

EVALUATION RESULTS

The product SolarWinds Orion Suite for Federal Government v3.0 has been evaluated against the Security Target SolarWinds Orion Software Security Target, version 1.12, July 16, 2018.

All the assurance components required by the evaluation level EAL2+ALC_FLR.2 have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2+ALC_FLR.2, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Applus Laboratories, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[ST] SolarWinds Orion Software Security Target, version 1.12, July 16, 2018.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: SolarWinds Orion Software Security Target, version 1.12, July 16, 2018.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.