MINISTERIO DE LA PRESIDENCIA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF: 2015-26-INF-1738 v1	Created by: CERT10
Target: Expediente	Revised by: CALIDAD
Date: 19.10.2016	Approved by: TECNICO

CERTIFICATION REPORT

File: 2015-26 SolarWinds Orion Suite for Federal Government v1.1

Applicant: SolarWinds Worldwide, LLC

References:

[EXT-2826] Certification request of Solarwinds Orion v1.1

[EXT-3172] Evaluation Technical Report of Solarwinds Orion v1.1.

The product documentation referenced in the above documents.

Certification report of the product SolarWinds Orion Suite for Federal Government V1.1, as requested in [EXT-2826] dated 14/10/2015, and evaluated by the laboratory Applus LGAI Technological Center S.A., as detailed in the Evaluation Technical Report [EXT-3172] received on 07/10/2016.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product SolarWinds Orion Suite for Federal Government v1.1.

The SolarWinds Orion 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 LGAI Technological Center S.A..

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R4 - EAL2+ALC_FLR.2.

Evaluation end date: 06 October 2016.

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 LGAI Technological Center S.A. 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 R4 and the CEM v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product SolarWinds Orion Suite for Federal Government V1.1, a positive resolution is proposed.

TOE SUMMARY4

The Orion 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. Application programs to manage FoE (Failover Engine) operations may also be invoked from the Windows Start menu by authorized users.

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 R4.

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	AVA_VAN.2. Vulnerability analysis

assessment	

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4:

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
FPT: Protection of the TSF	FPT_FLS.1. Fail secure
FRU: Resource utilisation	FRU_FLT.2. Fault tolerance
FTA: TOE access	FTA_SSL.3. Session locking and termination

IDENTIFICATION

Product: SolarWinds Orion Suite for Federal Government v1.1

Security Target: SolarWinds Orion Software Security Target, version 1.8, July 4, 2016.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R4 - EAL2 + ALC_FLR.2.

SECURITY POLICIES

The use of the product SolarWinds Orion Suite for Federal Government v1.1 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target. In short, it establishes the need of implementing organisational policies related to the following aspects.

Policy 01: P.ACCACT

Users of the TOE shall be accountable for their actions within the TOE.

Policy 02: P.ACCESS

All data collected and produced by the TOE shall only be used for authorized purposes.

Policy 03: P.ANALYZ

Analytical processes and information to derive conclusions about element or network problems must be applied to data received from managed elements and appropriate notification to users generated.

Policy 04: P.DBMONITOR

The Administrator shall monitor disk space usage of the databases used by the TOE and take proactive steps to protect against data loss. The TOE will be configured to monitor the databases and alert the Administrator to high disk usage levels.

Policy 05: P.DISCLOSURE

Credentials passed between the TOE and remote users will be protected from disclosure.

Policy 06: P.HIGHAVAIL

The TOE shall be able to continue providing all of its functionality to authorized users in a secure manner in the event of a failure of a single TOE component.

Policy 07: P.INTGTY

Data collected and produced by the TOE shall be protected from modification.

Policy 08: P.MANAGE

The TOE shall only be managed by authorized users.

Policy 09: P.PASSWORDS

Passwords for User Accounts defined in the TOE are only configured by Administrators.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following 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.

Assumption 01: A.ACCESS

The TOE has access to all the IT System data it needs to perform its functions.

Assumption 02: A.ASCOPE

The TOE is appropriately scalable to the IT Systems the TOE monitors.

Assumption 03: A.DATABASE

Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.

Assumption 04: A.ENVIRON

The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.

Assumption 05: A. INSTALL

The Administrator will install and configure the TOE according to the administrator guidance.

Assumption 06: A.NETWORK

There will be a network that supports communication between distributed components of the TOE. This network functions properly.

Assumption 07: A.NOEVILADMIN

Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product SolarWinds Orion Suite for Federal Government v1.1, 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.

The threats covered by the security properties of the TOE are categorized below.

Threat 01: T.INTERCEPT

An unauthorized network entity may intercept data exchanged between distributed TOE components to compromise the operation of the TOE or gain unauthorized access to TSF data.

Threat 02: T.MASQUERADE

A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.

Threat 03: T.TSF_COMPROMISE

A user or process may cause, through an unsophisticated attack, TSF data to be modified.

Threat 04: T.UNIDENT_ACTIONS

The administrator may not have the ability to notice potential security violations such as attempts by users to gain unauthorized access to the TOE, thus limiting the administrator's ability to identify and take action against a possible security breach.

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 categorized below.

Environment objective 01: OE.COMM

The Operational Environment will protect communication between the TOE and systems outside the TOE boundary from disclosure.

Environment objective 02: OE.CRYPTO

The Operational Environment will provide cryptographic functionality needed to provide confidentiality with the protocols used for communication with remote IT Systems.

Environment objective 03: OE.DATABASE

Those responsible for the TOE must ensure that access to the TOE database via mechanisms outside the TOE boundary (e.g., DBMS) is restricted to authorized users only.

Environment objective 04: OE.DBMONITOR

The Administrator shall monitor disk space usage of the databases used by the TOE and take proactive steps to protect against data loss. The TOE will be configured to monitor the databases and alert the Administrator to high disk usage levels.

Environment objective 05: OE.ENVIRON

The Administrator will install the TOE in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.

Environment objective 06: OE.INSTALL

The Administrator will install and configure the TOE according to the administrator guidance.

Environment objective 07: OE.INTROP

The TOE is interoperable with the IT Systems it monitors.

Environment objective 08: OE.NETWOKR

The Administrator will install and configure a network that supports communication between the distributed TOE components. The administrator will ensure that this network functions properly.

Environment objective 09: OE.NOEVILADMIN

Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.

Environment objective 10: OE.SSL

The Operational Environment will require incoming connections to the Orion Web Console and EOC Web Console to use SSL/TLS.

Environment objective 11: OE.TIME

The Operational Environment will provide reliable timestamps.

Environment objective 12: OE.WINDOWSACCESS

Users invoking the Orion Server functionality via Windows application programs must successfully perform identification and authentication functions with Windows first, and access to the applications that invoke ORION Server functionality must be limited to users authorized to invoke TOE management functionality.

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 three categories:

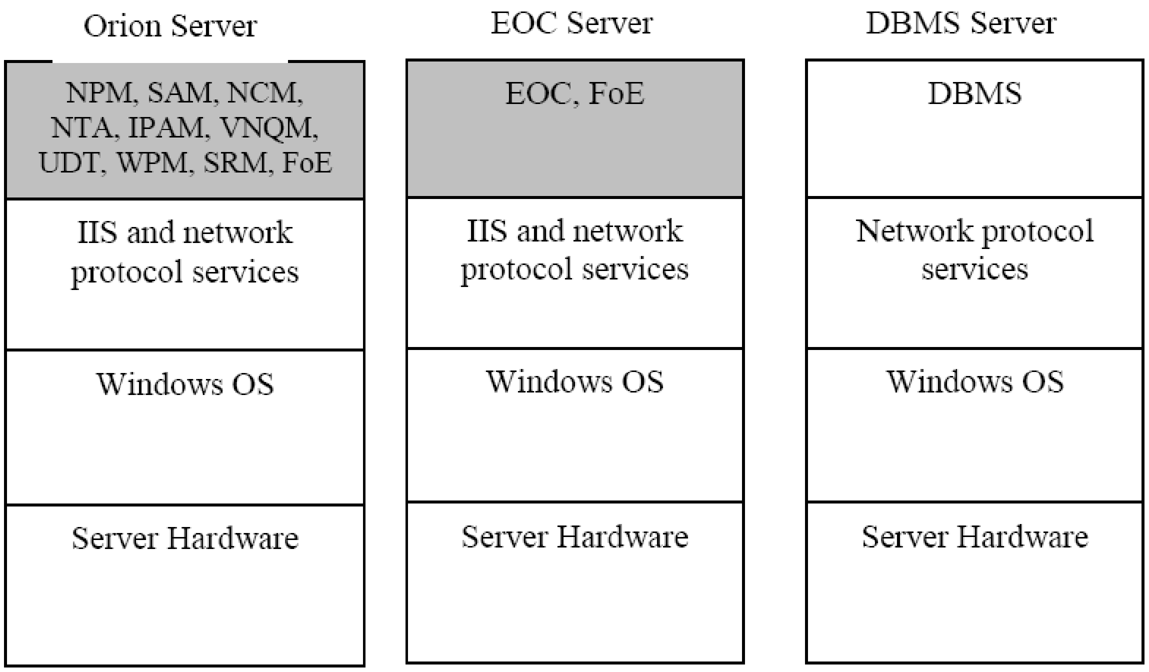
1. Orion monitoring and management subsystems (consisting of the subsystems associated with NPM, SAM, NCM, NTA, IPAM, VNQM, UDT, SRM, and WPM).
2. The FoE subsystem for monitoring and synchronizing of EOC and/or Orion applications and servers
3. EOC subsystems for aggregation of information from multiple Orion Servers

PHYSICAL ARCHITECTURE

The TOE consists of the SolarWinds Orion software identified in section 1.2 executing on multiple dedicated Windows servers:

1. EOC Server - EOC installed on a dedicated server.
2. Orion Server - Orion Suite components (other than EOC) installed on a dedicated server. Any combination of components may be installed with each instance. Any combination is generically referred to as an Orion Server.
3. Failover Server – FoE components are installed on a dedicated secondary server(s) as well as on primary EOC Servers or Orion Servers. The passive server monitors the health of the active EOC Server or Orion Server, and the passive server automatically assumes the active role of any failed server. The components on the active EOC Server or Orion Server ensure that data files required by the passive EOC Server or Orion Server are supplied to the passive server for replication.

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.


Orion Server
EOC Server
DBMS Server
NPM, SAM, NCM, NTA, IPAM, VNQM, UDT, WPM, SRM, FoE
EOC, FoE
DBMS
IIS and network protocol services
IIS and network protocol services
Network protocol services
Windows OS
Windows OS
Windows OS
Server Hardware
Server Hardware
Server Hardware

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 Administrator Guide (OrionEOCAdministratorGuide.pdf)
2. SolarWinds® Orion® Common Components Administrator Guide (OrionCoreAdministratorGuide.pdf)
3. SolarWinds® Orion® Network Performance Monitor Administrator Guide (OrionNPMAdministratorGuide.pdf)
4. SolarWinds® Server & Application Monitor Administrator Guide (SAMAdminGuide.pdf)
5. SolarWinds® Network Configuration Manager Administrator Guide (OrionNCMAdministratorGuide.pdf)
6. SolarWinds® IP Address Manager Administrator Guide (OrionIPAMAdministratorGuide.pdf)
7. SolarWinds® NetFlow Traffic Analyzer Administrator Guide (NetFlowAdministratorGuide.pdf)

8. SolarWinds® User Device Tracker Administrator Guide (UDTAdministratorGuide.pdf)
9. SolarWinds® Orion® VoIP and Network Quality Manager Administrator Guide (VNQMAdministratorGuide.pdf)
10. SolarWinds® Web Performance Monitor Administrator Guide (WPMAdminGuide.pdf)
11. SolarWinds Storage Resource Monitor Help Guide (SRMHelpGuide.pdf)
12. SolarWinds® Failover Engine v6.7 Administrator Guide (OrionFailoverEngineAdministratorGuide.pdf)
13. SolarWinds® Technical Reference Orion® Failover Installation Walkthrough (Failoverinstallwalkthrough.pdf)
14. SolarWinds® Technical Reference Preparing an Orion® Failover Engine Installation (PreparingOrionFailoverEngineInstallation.pdf)
15. SolarWinds® Orion® Suite for Federal Government Version 1.1 Common Criteria Supplement (OrionCommonCriteriaSupplement.pdf)

All guidance documentation is distributed as PDF files. Core product guidance documentation (items 1 through 12 above) is distributed within the component download files. Technical References (items 13 and 14 above) are downloaded from the Knowledgebase of the SolarWinds Customer Portal.

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 one (Orion Report Writer) and all the SFRs except for FTA_SSL.3, however this TSFI and SFR have been tested as part 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 identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests were developed using the testing scenario appropriate to the architecture defined 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 executed a set of test over a sampling of the developer's testing plan by considering the following factors:

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

In terms of security, the approach taken has been to prioritize the coverage of SFRs that have not been tested or that have a big implication in the overall security of the TSF data.

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 v1.1 it is necessary the disposition of the following software components:

- Orion Network Performance Monitor v11.5.2 with NPM-v11.5.2-CCC-HotFix.
- Orion Server & Application Monitor v6.2.2.
- Orion Network Configuration Manager v7.4.0.
- Orion NetFlow Traffic Analyzer v4.1.1.
- Orion IP Address Manager v4.3.0.
- Orion Voice & Network Quality Manager v4.2.2.
- Orion User Device Tracker v3.2.2.
- Orion Web Performance Monitor v2.2.0.
- Orion Storage Resource Monitor v6.2.0.
- Orion Enterprise Operations Console v1.6.2.
- Orion Failover Engine v6.7.0.

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 is the following:

1. EOC Server - EOC installed on a dedicated physical server. EOC installed on a dedicated server includes the Orion Enterprise Operations Console (EOC) V1.6.2 and Orion Failover Engine (FoE) V6.7.0.
2. Orion Server - Orion installed on a dedicated physical server with all the components included within the scope of the evaluation (except for EOC): SolarWinds Orion Network Performance Monitor (NPM) V11.5.2, Orion Server

& Application Monitor (SAM) V6.2.2, Orion Network Configuration Manager (NCM) V7.4.0, Orion Netflow Traffic Analyzer (NTA) V4.1.1, Orion IP Address Manager (IPAM) V4.3.0, Orion VoIP & Network Quality Manager (VNQM) V4.2.2, Orion User Device Tracker (UDT) V3.2.2, Orion Web Performance Monitor (WPM) V2.2.0, Orion Storage Resource Monitor (SRM) V6.2.0 and Orion Failover Engine (FoE) V6.7.0.

3. DB server. DMBS installed on a dedicated physical server. The specifications of the three mentioned physical server are identical (except the RAM memory of the Orion server) and they are shown in the table below.

Item	**Specification**
Operating System	Windows Server 2012 R2 64 bits
Web Server	IIS 8.5, SSL required
CPU	I5-4570 @ 3.2 GHz
RAM memory	8 GB (except for Orion server that has 10 GB)
Secondary memory	465 GB

EVALUATION RESULTS

The product SolarWinds Orion Suite for Federal Government v1.1 has been evaluated against the Security Target SolarWinds Orion Software Security Target, version 1.8, July 4, 2016.

All the assurance components required by the evaluation level EAL2 + ALC_FLR.2 have been assigned a “PASS” verdict. Consequently, the laboratory Applus LGAI Technological Center S.A. 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 R4 and the CEM v3.1 R4.

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 SolarWinds Orion Suite for Federal Government v1.1, 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, R4 Final, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, September 2012.

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 1.8, July 4, 2016.