Reference: 2021-42-INF-4015- v1
Target: Pública
Date: 16.05.2023

Created by: I006
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2021-42**
TOE	**Alteon version 32.6.3.50**
Applicant	**520044371 - Radware, LTD.**

References

[EXT-7298] 2021-08-06_2021-42_solicitud_certificacion

[EXT-8041] 2022-10-17_2021-42_ETR_vM0

Certification report of the product Alteon version 32.6.3.50, as requested in [EXT-7298] dated 06/08/2021, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-7298] received on 17/10/2022.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Alteon version 32.6.3.50.

Alteon is Radware's next-generation Application Delivery Controller (ADC) and the only network load balancer that guarantees application Service Level Agreement (SLA). It provides advanced, end-to-end local and global load balancing capabilities for all Web, cloud and mobile-based applications.

Developer/manufacturer: Radware, LTD.

Sponsor: Radware, LTD.

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

ITSEF: Applus Laboratories.

Protection Profile: No.

Evaluation Level: EAL 2

Evaluation end date: 03/03/2023

Expiration Date[1]: 03/05/2028

All the assurance components required by the evaluation level EAL 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 EAL 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 Alteon version 32.6.3.50, a positive resolution is proposed.

TOE SUMMARY

The TOE is the Alteon version 32.6.3.50 series of products, with the TSF covering the core load balancing capabilities together with the SSL Offloading and part of the management capabilities. The TOE, thus, acts as a load balancer which redirects service request in a balanced way to multiple providing servers. As such, from hence forward the TOE may be referred as an ADC or as a load balancer interchangeably. Additionally, the TOE provides the following major security features:

- Security Audit

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL 2, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5. Details of security functional requirements can be found in section 6 of the Security Target [ST]:

SECURITY FUNCTIONAL REQUIREMENTS
FAU_GEN.1
FAU_GEN.2
FAU_STG.1
FAU_STG.4
FCS_CKM.2
FCS_CKM.4
FCS_HTS.1
FCS_TLS.1/WBM
FCS_TLS.1/DATA
FCS_TLS.2
FDP_IFC.1
FDP_IFF.1
FIA_AFL.1
FIA_UAU.2
FIA_UID.2
FMT_MSA.1
FMT_MSA.3
FMT_SMF.1
FMT_SMR.2
FPT_STM.1
FTA_SSL.3
FTA_SSL.4
FTP_ITC.1
FTP_TRP.1

IDENTIFICATION

Product: Alteon version 32.6.3.50

Security Target: Alteon Security target, version 1.8, October 06 2022.

Protection Profile: No.

Evaluation Level: EAL 2

SECURITY POLICIES

The use of the product Alteon version 32.6.3.50 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, section 4.3 ("Organizational Policies").

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.

The detail of these assumptions is documented in the Security Target, section 4.4 ("Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Alteon version 32.6.3.50, although the agents implementing attacks have the attack potential according to the "Basic" of EAL 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 those defined in the Security Target, section 4.2 ("Threats").

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 those defined in the Protection Profile and they are documented in the Security Target, section 5.2 ("Security Objectives for the operational Environment").

ARCHITECTURE

LOGICAL ARCHITECTURE

As described in the Product Introduction and TOE Overview of the Security Target, the TOE is an application delivery controller whose main purpose is to act as a load balancer. From the major features outlined in the Product Introduction only the following ones are part of the logical scope:

- Server Load Balancing for the core function.
- SSL Offloading for providing application layer analysis capabilities.
- Management Capabilities for managing the configuration and access control.

The TSF is grouped in the following categories:

- SECURITY AUDIT

  The TOE generates audit records for security-related events across its multiple functional module which are then stored in the local storage. The audit logs are protected from unauthorized modification and deletion.

- CRYPTOGRAPHIC SUPPORT

  The TOE protects the confidentiality and integrity of all of the information passed between the TOE and the authorized administrators, the service clients and the back end servers. The TOE protects these communications by implementing the TLS secure transport protocol.

- USER DATA PROTECTION

  The TOE achieves information flow control applying different policies and rules to the traffic that passes through its data path interfaces (INGRESS AND EGRESS PORTS). Information flow control is used by the TOE to load balance service requests to back end servers in accordance with the rules configured by the administrator.

- IDENTIFICATION AND AUTHENTICATION

  The TOE requires that the users have an associated role, and that they must be identified and authenticated before granting them access to the TOE and its security functions. Users can authenticate through the Web Management interface (HTTPS) using their username and password.

- SECURITY MANAGEMENT

  The TOE provides remote management capabilities via Web Management interface (HTTPS). The security management functionality allows the administrators to configure users, roles and all of the other configuration objects (servers, virtual services, SSL policies, etc.) used in the creation and management of the load balancing rules.

- PROTECTION OF THE TSF

The TOE provides reliable internal timestamps in order to support the audit functionality.

- TOE ACCESS

  The TOE allows user-initiated and automatic session termination for its Web Management interface (HTTPS). This feature reduces the risk of an attacker using an administrator open session.

- TRUSTED PATH/CHANNELS

  The channels established between the TOE and its remote administrators are protected using TLS1.3 for the Web Management Interface (HTTPS). Meanwhile, the channels used for communicating between the TOE and the clients/servers is protected using TLS1.2 and TLS1.3, as per mandated in the evaluated configuration.

PHYSICAL ARCHITECTURE

The TOE consists of a Software Alteon 32.6.3.50 deployed in a Virtualized Platform or Alteon Hardware Appliance.

The virtual appliances (VA) correspond to images used to deploy virtual machines containing the Alteon software. The VAs always come as a complete singular Alteon instance and therefore, only one image is provided for each supported platform.

File Name	**Virtualization Platform**	**SHA-256**
AlteonOS-32.6.3.50_rls_74.ova	VMWare VA	d8a9b0fd1228c5ca65fe9d4bad7e0eff781a81942652a822eed5b9005bea0a33
AlteonOS-32.6.3.50_rls_74_xen.tgz	Xen VA	fced85f91a51e9f67efdf2e640b166a391f34b28a0ae9275db5f4dd43e79ea93
AlteonOS-32.6.3.50_rls_74.qcow2	KVM-VA (OpenStack)	576aeb728a671b21a20d4a13c35a7359be785576e738ea090ce94d9abf863d2b
AlteonOS-32.6.3.50_rls_74_kvm.tgz	KVM VA	6159fc304fc3c909e10036a7847e7f1df94aea2a6d1b094d7e02fa174fd376eb

The supported physical appliances, these are Alteon Hardware products indicated in the Security Target.

All these physical appliances don’t include the correct version of the TOE hence when the appliance is received, the end user must perform an upgrade process in order to upgrade the TOE to its correct version. Radware maintains a single code base where all of the product features (TSF included) are implemented. The code base is then compiled and packaged specifically for each of the supported underlying platforms, resulting in multiple images. Thus, any change to the code base is observable and applicable to all platforms, guaranteeing the complete equivalency at the functional and security level.

Since the Alteon image for standalone deployment mode contains all of the necessary application for upgrading the form factors ADC and ADC-VX, the following table contains a full list of images that are provided in the IMG format for both deployment modes (Standalone and ADC-VX) and can be used to upgrade Alteon series of products. Additionally, the following table define for each type of Alteon Hardware its corresponding image in order to be upgraded.

File Name	Alteon Hardware Appliance	SHA-256
AlteonOS-32.6.3.50-5k.6k.8k_rls_74_qat.img	Alteon 6420 S Alteon 8420 S Alteon 8820 S	acbaf32461f80d422edad451d02972cd38ad4dca0ff95663a796a94d6ea03247
AlteonOS-32.6.3.50-DPDK_rls_74.img	Alteon 7220 S Alteon 7612 S Alteon 9800 Alteon D-5208 Alteon D-5424 S Alteon D-5820 S	ef41036bf3cd0d9ce2c12d69afaf17282d50dbf5b53f4ba3ff9bc2a3cebacca2

DOCUMENTS

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

Document Name	Document ID	SHA-256
Alteon CLI Application Guide	RDWR-ALOS-V3263_CLIAG2012	f3bdf9990c6ddcd0f00da155fc148c15eb1f8d543b21c338e0ec77ee5e1ec70f
Alteon Getting Started Guide	RDWR-ALOS-V3263_WBMGS2012	b1e97e8f7cff67c149434abb3f282172d23a1ee01366cb48ecaf1245b3b3cef2

Alteon WBM Application Guide	RDWR-ALOS-V3263_WBMAG2012	a3a1b3612cb458ccd7e4438cc3dd5fd9129ee063861ab5916bd14df42915bd90
Alteon VA Installation and Maintenance Guide	RDWR-ALOS-V3263_VA_IG2012	fa8392f97cc038bc9eeb89b4c324224af0319552511fa0c1bf488d7492174709
Alteon Installation and Maintenance Guide	RDWR-ALOS-V3263_IG2012	0dec82b544be6a63c07457d65259e9ba0cd1feb3e427e1f4741ed412ddf6e1cc

PRODUCT TESTING

The developer has executed test for all the security functions. 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.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises. Likewise, he has selected and repeated about 25% of the developer functional tests in the testing platform implemented in the evaluation laboratory, selecting one test for each of the most relevant functional class.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Alteon version 32.6.3.50 it is necessary the disposition of the following software and hardware components:

- For bare-metal installations, at least one appliances from the following line is required:

  - Alteon 6420 S
  - Alteon 8420 S
  - Alteon 8820 S
  - Alteon 7220 S
  - Alteon 7612 S
  - Alteon 9800
  - Alteon D-5208
  - Alteon D-5424 S
  - Alteon D-5820 S

- For virtual appliances (VA) installations, the following minimum requirements apply:
  - vCPU: 1
  - RAM: 2GB
  - Disk space: 7GB
  - Virtualization Platform:
    - VMWare ESXi
    - KVM
    - Xen
    - KVM (OpenStack)

  The VAs is built specifically for specific virtualization platform, for example OVA files are used in VMWare ESXi platform while the image for the KVM platform is an qcow2 or tgz file. For more details on supported hardware and their configuration see the Alteon VA Installation Guide.

- Web Browser
  - Chrome
  - Firefox
  - MS Edge

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the evaluation is the following:

- Client 1:
  - OS: Ubuntu 18.04.

  - Description: This device will be used to access to the services offered by the servers in the Back-end network. The IP address for this computer may vary, the only requirement will be that its IP address is within the Client Network IP range.

- Client 2:
  - OS: Kali Linux 2020.4.
  - Description: This device will be used to access to the services offered by the servers in the Back-end network. The IP address for this computer may vary, the only requirement will be that its IP address is within the Client Network IP range.
- Alteon: A valid bare-metal or hypervisor running the Alteon 32.6.3.50 TOE. The list of valid bare-metal appliances and Hypervisors can be found in the Security Target. The tests defined along this document have been performed using a VMWare ESXi 6.7 hypervisor. This device will be connected to the Client and Back-End networks through its datapath interfaces and with the Administration Network through its Management Interface.
- Administration PC:
  - OS: Kali Linux 2020.4.
  - Description: This device will be used to access to the management interfaces of the TOE. The IP address for this computer may vary, the only requirement will be that its IP address is within the Administration Netwok IP range.
- Server 1:
  - OS: Ubuntu 18.04
  - Description: This device will be running an Apache 2.4.29 service which will be exposed through its Back-End Network interface.
- Server 2:
  - OS: Ubuntu 18.04
  - Description: This device will be running an Apache 2.4.29 service which will be exposed through its Back-End Network interface.

EVALUATION RESULTS

The product Alteon version 32.6.3.50 has been evaluated against the Security Target Alteon-Security-Target-v1.8

All the assurance components required by the evaluation level EAL 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 EAL 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.

There is no additional recommendation from the Laboratory in order to use the TOE since guidance documentation is enough to make a secure usage of the TOE.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Alteon version 32.6.3.50, a positive resolution is proposed.

The certifier recommends potential TOE consumers to observe Evaluation Team recommendations, strictly following the TOE guidance referenced in section DOCUMENTS and to analyse the assumptions defined in the security problem definition in section 3 of the [ST].

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
ST	Security Target

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]

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- Alteon Security Target, version 1.8, October 2022

RECOGNITION AGREEMENTS

In order to avoid multiple certifications 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.eu.

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 CCRA for all assurance components selected.