TÜVRheinland®
Precisely Right.

Certification Report

NetNumen U31 R13 V12.11.10 Element Management System (EMS) on Linux/HP

Sponsor and developer: ***ZTE Corporation***
NO. 55 Hi-tech Road South
ShenZhen
518057, P.R.China

Evaluation facility: ***Brightsight***
Delftechpark 1
2628 XJ Delft
The Netherlands

Report number: **NSCIB-CC-10-10153-CR**

Report version: **1**

Project number: **NSCIB-CC-10-10153**

Authors(s): **Denise Cater**

Date: **April 18, 2011**

Number of pages: **14**

Number of appendices: **0**

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 3 (ISO/IEC 15408)
Certificate number	**C11-10153**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**ZTE Corporation** **Located in ShenZhen, P.R.China**
Product and assurance level	**NetNumen U31 R13 V12.11.10 Element Management System (EMS) for Linux/HP** Assurance Package: ▪ EAL2 augmented with ALC_FLR.2
Project number	**NSCIB-CC-10-10153**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 3 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 3 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 3. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity

Date of issue : **18-04-2011**

Certificate expiry : **18-04-2021**

Registration number
Notified Body 0336

PRODUCTS
RvA C078
Accredited by the Dutch Council for Accreditation

Managing Director
TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products.

A part of the procedure is the technical examination (evaluation) of the product according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

Recognition of the certificate

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NetNumen U31 R13 v12.11.10 Element Management System (EMS) on Linux/HP. The developer of the NetNumen U31 R13 is ZTE Corporation located in ShenZhen, P.R. China and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The Target of Evaluation – TOE (i.e., the NetNumen U31 R13 v12.11.10 Element Management System (EMS) on Linux/HP) is a telecommunications Element Management System plus client, which is used to manage a wireless telecommunications network. The EMS includes the server platform and an integrated CGS Linux kernel, and the client consists of a Java application.

The EMS is intended to be the highest management workstation for a certain supplier in a telecommunication network. It manages one or more Operation Maintenance Modules (OMMs, which manage a telecommunication network for a specific telecommunication technology such as CDMA or WiMAX) and provides information to the Network Management System (NMS) used by a network operator.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on 18 April 2011 with the delivery of the final ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*. The certification was completed on 18 April 2011 with the preparation of this Certification Report.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the NetNumen U31 R13, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the NetNumen U31 R13 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that it meets Evaluation Assurance Level 2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw reporting procedures). The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 3 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the NetNumen U31 R13 v12.11.10 Element Management System (EMS) on Linux/HP evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NetNumen U31 R13 v12.11.10 Element Management System (EMS) on Linux/HP, from ZTE Corporation located in ShenZhen, P.R. China.

This report pertains to the TOE comprised of the following main components:

Delivery item type	Identifier	Version	Medium
Hardware	HP BL460cG6, 2 E5504 CPUs, 8GB Memory, 2 300GB SAS Disks, SAS adapter and HP MSA2000sa G2 5 x HP 300GB SAS 15K 3.5"HDD; OR HP BL680cG5, 4 E7420 CPUs, 8GB Memory, 2 300GB SAS Disks, SAS adapter and HP MSA2000sa G2 5 x HP 300GB SAS 15K 3.5"HDD; OR HP BL680cG5, 4 E7420 CPUs, 16GBMemory, 2 300GB SAS Disks, SAS adapter and HP MSA2000sa G2 6 x HP 300GB SAS 15K 3.5"HDD; OR HP BL680cG5, 4 E7450 CPUs, 32GBMemory, 2 300GB SAS Disks, SAS adapter and HP MSA2000sa G2 8 x HP 300GB SAS 15K 3.5"HDD;	n/a	Server hardware
Software	EMS Client version NetNumen U31 R13	V12.11.10	Installed by ZTE engineer
	EMS Server version NetNumen U31 R13 (Linux)	V12.11.10	Installed by ZTE engineer
	Java(TM) SE Runtime Environment	build 1.6.0_21-b06	Installed by ZTE engineer
	Java HotSpot(TM) Client VM	build 17.0-b16, mixed mode	Installed by ZTE engineer
	CGS Linux	V3.02.00_P03/64bit	Installed by ZTE engineer
	Oracle for Linux	10.2.0.4 EE 64bit	Installed by ZTE engineer

To ensure secure usage a set of guidance documents is provided together with the NetNumen U31 R13. Details can be found in section 2.5 of this report.

2.2 Security Policy

The TOE is the NetNumen U31 R13 v12.11.10 Element Management System (EMS) on Linux/HP and is an Element Management System for a certain supplier in a telecommunication network that is used to manage one or more OMMs and provides information to the NMS (see below). The TOE communicates with these network entities using the IP protocol.

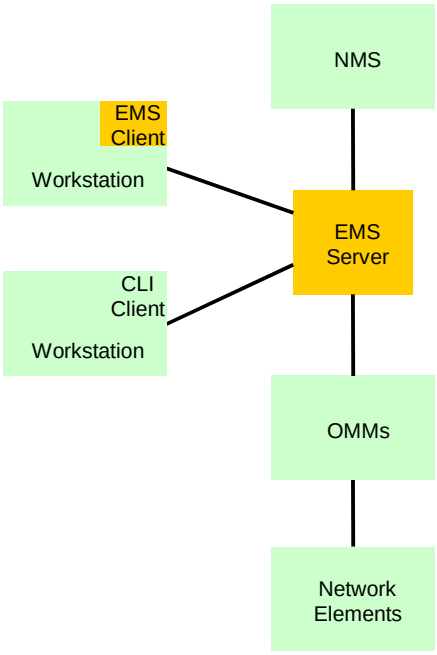

Figure 1 – Overview of the TOE in its environment

The security measures of the TOE aim at providing:

- A flexible role-based authorization framework with predefined and customizable roles. These roles can use the TOE to manage the wireless telecommunications network, and manage the TOE itself;
- A flexible authentication framework, allowing the TOE to accept/reject users based on: username/password and a configurable subset of IP/MAC-address and time of login;
- Flexible logging and auditing of events;
- Protected communication between EMS Server and the NMS, the OMMs the EMS Client and the CLI against masquerading, disclosure and modification.

2.3 Assumptions and Clarification of Scope

2.3.1 Usage assumptions

There are no usage assumptions identified in the Security Target that are of relevance to the TOE.

2.3.2 Environmental assumptions

The following assumption about the environmental aspects defined by the Security Target has to be met (for the detailed and precise definition of the assumption refer to the *[ST]*, chapter 3.3):

- The customer is responsible for ensuring the NMS and OMMs are trusted, and will not be used to attack the TOE. This means that the NMS and OMMs should be (logically and physically) protected appropriately.

Furthermore, the following organisational security policy relates to the environment in which the TOE shall be operated (for the detailed and precise definition of the organisational security policy refer to the *[ST]*, chapter 3.1):

- A flexible role-based authorization framework with predefined and customizable roles should be used to both manage the wireless telecommunications network, and manage the TOE itself. The customer should use this authorization framework to implement an organizational structure with different roles for the operators of each different wireless telecommunication network structure and different network technologies (such as CDMA, WiMAX).

2.3.3 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

Figure 2 presents the physical scope and boundaries of the TOE. The TOE consists of the following components:

- EMS Server hardware (HP server and disk arrary as detailed in chapter 2.1 of this document above) - Stores all data and SW, and runs all SW of the EMS Server;
- Operating System (CGS Linux Kernel) - Provides firewall, runs other SW on the EMS Server;
- EMS Server Software – Provides:
  - Unified Network Mgt. Application Platform: Performs authentication, authorisation and stores logging data. Handles all ssh, sftp, snmpv3 connections
  - Security Management: Configures the authentication and authorisation
  - Log Management: Configures logging, allows viewing of log
- Java SE Runtime Environment and Java Hotspot Client - Runs the EMS Server SW;
- Oracle for Linux - Arranges persistent data storage;
- EMS Client Software - GUI to the Server, provides ssh and sftp functionality.

The EMS Server is managed using either the EMS Client Software or from a CLI client (which forms part of the environment), both of which interact with the TOE over SSH. The EMS Client software also supports an SFTP interface for the download of large amounts of data from the EMS Server to the EMS Client.

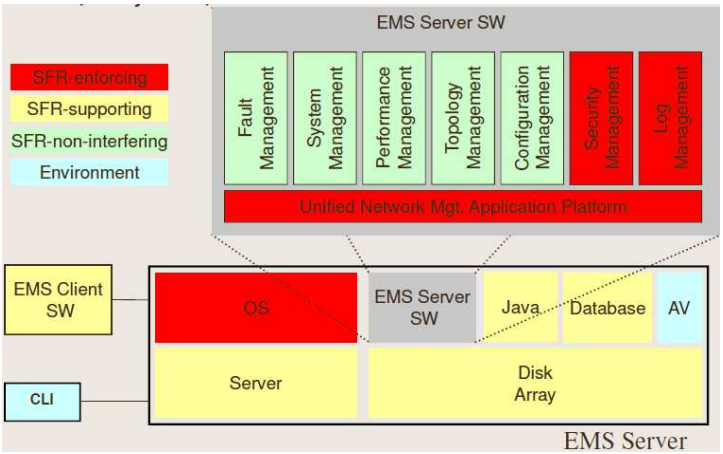

Figure 2 – The NetNumen U31 R13 physical and logical composition

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Standard Guidance:	
Network Element Management Technical Manual	V12.11.10 Revision 1.3
Network Element Management Security Management Manual	V12.11.10 Revision 1.2
Network Element Management Command Manual	V12.11.10 Revision 1.2
Maintenance:	
Network Element Management Routine Maintenance Manual	V12.11.10 Revision 1.2

Any additional guidance documentation that may be provided with the product is outside the scope of the evaluation, has therefore not been evaluated and does not contribute to the product in its certified form.

2.6 IT Product Testing

Testing (coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 2.6.1 Testing approach

The developer tested the TOE in the ST configuration Mode 4, as delivered to a customer, with one exception:

- A ssh port (22) was opened. This allowed direct access to the internals of the TOE for ease of access and testing

For these tests ZTE used a test suite that consists of a number of tests, each of which was performed manually. The developer used the EMS Client for all management of the EMS Server during testing.

The independent testing comprised of:

- Sample testing (2:ATE_IND.2-4) to validate the developer testing by repeating (4) developer's tests from the evaluator's site. The selected subset covers significant aspects of the SFRs.
- Independent testing (2:ATE_IND.2-6) was performed based on (9) new tests defined by the evaluator for the validation of the correct enforcement of all SFRs and an 'idle' test (to meet the requirements of [NSI6]). Seven of the tests were repeated following minor patching of the TOE by the developer in response to items raised by the evaluator.

2.6.2 Test Configuration

Independent testing was performed remotely (the TOE remained in China) on two testing setups:

- One "Practical" test-setup using Mode 4, to perform all tests except the Idle test;
- One "Idle" set-up using Mode 1, to perform the "Idle" test: this test setup was left idle for two weeks as one of the penetration tests, while the outgoing traffic of the EMS Server was measured.

2.6.3 Independent Penetration Testing

The evaluator independent penetration tests were conducted according to the following testing approach:

1. During evaluation of the ADV, ATE and AGD classes the evaluators hypothesized possible vulnerabilities. This resulted in a shortlist of possible vulnerabilities to be further analysed in AVA using the design knowledge gained. This resulted in a shortlist of potential vulnerabilities to be tested.
2. The evaluators used CEM Annex B.2 as an additional source for possible vulnerabilities and penetration tests.
3. The evaluators conducted a search of the public domain to identify any relevant vulnerabilities relating to components of the TOE. This resulted in a shortlist of possible vulnerabilities to be further analysed in AVA using the design knowledge gained. This resulted in a shortlist of potential vulnerabilities to be tested.
4. The short list was presented, under NSP#6, to the Scheme, and in discussion with the Scheme more penetration tests emerged.

As a result of the vulnerability analysis conducted, (26) penetration tests were performed to determine whether any potential vulnerabilities could be exploited in the operational environment, some of which were repeated following minor patching of the TOE by the developer in response to items raised by the evaluator.

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its ST and functional specification.

The "Idle" test used the tcpdump tool to record traffic initiated by the TOE over a two week period. Analysis of the traffic recorded in this test determined no unexpected traffic was initiated by the TOE by the TSFI covered in the Functional Specification.

No exploitable vulnerabilities or residual vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name, version number, integrated operating system and server hardware manufacturer NetNumen U31 R13 v12.11.10 Element Management System (EMS) on Linux/HP and can be identified by the version reported via the CLI and GUI.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references an ASE Intermediate Report and other evaluator documents. The verdict of each claimed assurance requirement is given in the following tables:

Development		**Pass**
Security architecture	ADV_ARC.1	Pass
Functional specification	ADV_FSP.2	Pass
TOE design	ADV_TDS.1	Pass

Guidance documents		**Pass**
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass

[2] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Life-cycle support		Pass
Configuration Management capabilities	ALC_CMC.2	Pass
Configuration Management scope	ALC_CMS.2	Pass
Delivery	ALC_DEL.1	Pass
Flaw Remediation	ALC_FLR.2	Pass

Security Target		Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass

Tests		Pass
Coverage	ATE_COV.1	Pass
Functional tests	ATE_FUN.1	Pass
Independent testing	ATE_IND.2	Pass

Vulnerability assessment		Pass
Vulnerability analysis	AVA_VAN.2	Pass

Based on the above evaluation results the evaluation lab concluded the NetNumen U31 R13 v12.11.10 Element Management System (EMS) on Linux/HP to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 2 augmented by ALC_FLR.2**. This implies that the product satisfies the security technical requirements specified in Security Target "NetNumen Network Element Management Security Target, Version: R13 V12.11.10 for Linux/HP, Revision 1.0, 05 April 2011". The Security Target does not claim conformance to any Protection Profile.

2.9 Evaluator Comments/Recommendations

2.9.1 Obligations and hints for the developer

None.

2.9.2 Recommendations and hints for the customer

Any additional guidance or functional specification documentation beyond that listed in section 2.5 that may be provided with the product to the customer is outside the scope of the evaluation, has not been evaluated and does not contribute to the product in its certified form.

The ZTE NetNumen U31 R13 V12.11.10 Element Management System (EMS) product is also available on Windows and Solaris platforms. These platforms have not been evaluated and are not covered by this certification report.

The customer should also pay attention to section 1.4 of *[ST]* that mentions that the antivirus software and the backup and disaster recovery option have not been evaluated and are not covered by this certification report.

3 Security Target

The Security Target “NetNumen Network Element Management Security Target, Version: R13 V12.11.10 for Linux/HP, Revision 1.0, 05 April 2011” is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

CC	Common Criteria
CDMA	Code-Division Multiple Access
EMS	Element Management System
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NMS	Network Management System
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
OMM	Operation Maintenance Module
PP	Protection Profile
TOE	Target of Evaluation
WiMAX	Worldwide Interoperability for Microwave Access

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I version 3.1 revision 1, and Part II and III, version 3.1 revision 3.
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 3, July 2009.
[ETR]	Evaluation Technical Report ZTE NetNumen U31 R13 v12.11.10 for Linux/HP, EAL2+, 11-RPT-082 v4.0, 12 April 2011
[NSCIB]	Nederlands Schema for Certification in the Area of IT Security, Version 1.2, 9 December 2004.
[NSI6]	NSCIB Scheme interpretation #6, Testing software TOEs on PC hardware platforms, Version 0.1, 18 November 2010
[NSP6]	NSCIB Scheme Procedure #6, Medium Assurance Evaluations, Version 0.4, 08 November 2010
[ST]	NetNumen Network Element Management Security Target, Version: R13 V12.11.10 for Linux/HP, Revision 1.0, 05 April 2011.

(This is the end of this report).