National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

BMC Software PATROL ® Perform/Predict
Version 6.5.30

Report Number: CCEVS-VR-02-0018
Dated: 8 April 2002
Version Number: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road, STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

David A. Wheeler
William R. Simpson
Institute for Defense Analyses
Alexandria, VA

Common Criteria Testing Laboratory

Computer Sciences Corporation
Annapolis Junction, MD

National Information Assurance Partnership

Common Criteria Certificate

BMC Software, Inc.

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: BMC Software PATROL® Perform/Predict
Version and Release Numbers: 6.5.30
Evaluation Platform: Sun Ultra 5 running Solaris 2.7 or Dell GX1 (PC) running Windows NT 4.0 SP6a
Assurance Level: EAL2

Name of CCTL: Computer Sciences Corporation
Validation Report Number: CCEVS-VR-02-0018
Date Issued: 8 April 2002
Protection Profile Identifier: N/A

Original Signed

Director
Information Technology Laboratory
National Institute of Standards and Technology

Original Signed

Information Assurance
Director
National Security Agency

1. Executive Summary

An evaluation of the BMC Software, PATROL ® Perform/Predict, Version 6.5.30, was begun 6 September 2001 and completed 27 March 2002. The evaluation was performed by Computer Sciences Corporation in the United States. The evaluation was carried out in accordance with requirements drawn from the Common Criteria CCv2.1, Part 3 for EAL2 [CC_PART3] and Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology [CEM_PART2]. The assurance activities in this level offer confidence that the BMC Software, PATROL ® Perform/Predict, Version 6.5.30 (with documentation and software deliverables as defined in sections 6. and 8., respectively) contains requirements that are:

- Justifiably included to counter stated threats and meet realistic security objectives,
- Internally consistent and coherent
- Technically sound and
- Free from vulnerabilities associated with obvious and known threats.

Computer Sciences Corporation, the Common Criteria Testing Laboratory [CCTL], is accredited by the National Voluntary Laboratory Accreditation and approved by the NIAP validation body to conduct Common Criteria evaluations. The CCTL has presented CEM work units and rationale that are consistent with the CC, the CEM and CCEVS publication number 4 Guidance to CCEVS Approved Common Criteria Testing Laboratories [CCEVS_PUB 4]. The CCTL team concluded that the requirements of the EAL 2 have been met. Therefore, a **pass** verdict has been issued, by the CCTL, for the BMC Software, PATROL ® Perform/Predict, Version 6.5.30. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

1.1. Evaluation Specific Details

Dates of Evaluation: 6 September 2001 - 27 March 2002
Evaluated Product: PATROL ® Perform/Predict, Version 6.5.30.
Developer: BMC Software Inc., 2101 City West Boulevard, Houston, TX 77042
CCTL: Computer Sciences Corporation
Evaluation Class: EAL2
Validation Team: David A. Wheeler, Institute for Defense Analyses
William R. Simpson, Institute for Defense Analyses

2. Product Identification

BMC Software, PATROL ® Perform/Predict, Version 6.5.30

3. Security Policy

There are no relevant security policies stated in the ST. It is the goal of the security function to prevent unauthorized startup of the data collection function.

4. Assumptions and Clarification of Scope

As with any evaluation, this evaluation shows that the evaluated configuration meets the security claims made, with a certain level of assurance. This evaluation did *not* evaluate the networking functions available in the commercial product—these functions are disabled in the evaluated configuration. It is also worth noting that the evaluated configuration is a special configuration that, after purchase, is installed and configured by the vendor at the customer's premises; this evaluation does not apply to the "standard" product that can be purchased and directly installed by customers. This ST only claims that unauthorized users cannot start the collection process (the process that gathers data about the system); it makes no claims that the collection process cannot be stopped, nor does it claim that the TOE protects the generated data. The product has been evaluated at the assurance level of EAL 2 that it meets its functional claims.

4.1 PATROL "system" Environmental Assumptions

This security target specifies the following usage assumptions for the TOE environment:

Name	Description
A.ACCESS_CONTROL	The underlying operating systems of Perform/Predict are configured to provide discretionary access control (DAC) to Perform/Predict executables and data files per site policy. *
A.MANAGE	There are one or more competent individuals assigned to manage the TOE. Those assigned to manage the TOE have been appropriately trained.
A.NOEVIL	Administrators are not careless, willfully negligent, nor hostile; and will follow and abide by all administrator guidance; however, they are capable of error.
A.OPERATE_CORRECT	The computer platforms and operating systems software operate correctly.
A.PHYSICAL_PROTECT	The processing resources of the TOE will be located within facilities providing controlled access to prevent unauthorized physical access.

*APPLICATION NOTE: The underlying operating system provides discretionary access control to protect the authorization.cfg file from modification by users and prevents unauthorized users from accessing the Perform/Predict installation directory and its contents. These assumptions require that the underlying operating system possess the notion of users and groups along with user and group access permissions. These operating system features are present in the evaluated configuration.

4.2 Clarification of Scope

This is a limited security functionality product evaluated at EAL2 that counters the sole threat of unauthorized start of the data collection function.

4.2.1 Interpretations

There are no national interpretations of the U.S. Scheme or international interpretations that apply to this evaluation.

4.2.2 Threats

Specific threats to IT security that should be countered by the BMC Software, PATROL ® Perform/Predict, Version 6.5.30.

Name	Description
T.UNAUTH_USAGE	Hostile/unauthorized users with limited attack potential could instantiate a TOE collection process, which could result in the loss of integrity of the collected data.

4.2.3 Security Content of the Product

The security content of the product is limited, Namely, the TOE and the environment may jointly provide the following security functionality:

- Protection of the ability to prevent unauthorized startup on the collection function.

5. Architectural Information

```
BMC Software, PATROL ® Perform/Predict, Version 6.5.30, is a
set of software tools designed to assist in measuring,
evaluating, predicting, and reporting the performance and
capacity of distributed systems. The TOE configuration
consists of 6 software components:
          a) Manager
          b) Collect
```

c) UDRprovider
d) Analyze
e) Predict
f) Visualizer

Of these components, only the UDRprovider offers any security functionality. The Manager, Predict, Visualizer, and Analyze components only allow for the analysis of collected data. Since these components do not implement any security functions, they are not part of the TOE Security Functions (TSF) and the design of these portions of the TOE will not be further described.

UDRprovider executes in either of the following environments: a Sun running Solaris 2.6-2.7, or an x86 running Windows NT with a minimum of Service Pack 5 (SP5). BMC Software, PATROL ® Perform/Predict, Version 6.5.30 Evaluation Technical Report Perform/Predict, Version 6.5.30 provides the following TOE security functions:

- User Data Protection (FDP).
- Security Management (FMT).

The IT Environment provides the following security function:

- Identification and Authentication (FIA).

Perform/Predict provides a methodology for the authorization of users on each node. The authorization.cfg file on each node that UDR Provider and Collect are on is used by UDRprovider to validate a user's (the user's identity is established through the Identification and Authentication (FIA) mechanism provided by the IT environment) authority to start the collection process (FIA and FDP). The default permission grants all users full authorization to all information, however, this file can be edited on a per-user basis by assigning any of four permission levels: *manag*e, *modify*, *vie*w, or *none* (FMT). NOTE: In the evaluated configuration, *view* and *none* are not applicable because they have no functionality within the secure configuration.

6. Documentation

The documentation provided with the product is as follows:

[PP-001a]	BMC 6.5.30 NT and Unix Release Notes (email dated:1/23/01) plus mkPATROL for NT Performance Information for 6.5.30 Release Notes/NT Manager and Secure Nodes, 3/8/2001
[PP-001b]	BMC PATROL for Unix Performance Information for 6.5.30 Release Notes/Unix Manager and Secure Nodes, 3/8/2001
[PP-002a]	BMC PATROL for Microsoft Windows 2000 Servers, Release Notes Version 6.5.30 1/29/01, dated 2/5/2001

[PP-002b] BMC PATROL RTM for Unix Performance Release Notes, Version6.5.30, 1/29/01, dated 2/5/2001

[PP-003] BMC PATROL for Unix Performance Getting Started, dated 1/10/2001

[PP-004] BMC Software Configuration Management Document for Security, dated 6/11/2001

[PP-005] BMC Product Packaging and Delivery Procedures for PATROL Classic, PATROL Enterprise Manager, and PATROL Perform/Predict, dated 9/7/2001

[PP-006] BMC Software, PATROL Perform/Predict, Version 6.5.30 Design Document, dated 2/2/2002

[PP-007] BMC Software, PATROL Perform/Predict, Version 6.5.30 Security Target, dated 1/24/2002

[PP-008] BMC Security Test Document for Perform/Predict Product Version 6.5.30, dated1/24/2002

[PP-009] BMC Software, PATROL Perform/Predict, Version 6.5.30 Vulnerability Assessment, dated 1/29//2002

[PP-010] BMC Authorization Test Cases, dated 3/8/2002

[PP-011] BMC Technical Bulletin, dated3/8/2002

7. IT Product Testing

EAL2 provides for minimal testing, including review of developer tests (with some confirmation) and minimal independent security functional testing. There is no automated test suite executed for this level of assurance.

7.1 Test Goals

This testing is being performed as an augmentation to developer testing of the TSF of the TOE.

7.2 Test Approach

The tests included herein do not require any automated test suite. This test will be manually performed with step-by-step instructions. For the work packages ATE_IND.2-4 through ATE_IND.2-8 the evaluation teams test subset is based on the following:

> Whereas the TOE has only one TOE security function, and the developer's tests clearly exercise the access control functionality provided through the *Authorization.cfg* file. The evaluator's therefore focused on the major change in this version of the Product from previous versions. This change is manifested in the removal of the network connectivity function(s) of the previous versions.

For the ATE_IND.2-9 and ATE_IND.2-10 work units, the evaluators selected three scenarios. The first was to test that the TOE functioned (correctness of collection data was not considered a security relevant issue) given no access control mechanism in the *Authorization.cfg* file. The second and third were to validate on each platform that a user not listed in the *Authorization.cfg* file could not start a collection.

7.3 Test Configuration

The TOE is to be installed by BMC at the customer site. A BMC engineer as required performed the installation. As the only security related function is contained in the Perform/Predict product resides in the authorization.cfg file, the agent was loaded on two machines only. The physical configuration consisted of the two platforms networked together on a simple LAN using an Ethernet hub. All tests were conducted with the default configuration listed in section 8.

8. Evaluated Product Configuration

8.1 Software Configuration

The BPP_ST_0.1, BPP_SCM_1.08 show the Physical TOE as consisting of:

> BMC Software PATROL Ò Perform/Predict, version 6.5.30 components:
>
> Manager 6.5.30
> Collect 6.5.30
> UDRprovider 6.5.30
> Analyze 6.5.30
> Predict 6.5.30
> Visualizer 3.5.04 (windows only)

The logical TOE consist only of:

> UDRprovider 6.5.30

Of these components only UDRprovider has security functionality. The Manager, Predict, Visualizer and Analyze components are run on a separate computer and allow only for the data collected, they have no security functionality. The media is controlled and installed by BMC.

8.2 Hardware Configuration

No hardware is provided with the deliverable. The following hardware configurations were evaluated:

System	Configuration	Tools/Services	Accounts
Hephaestus 192.168.0.125	P2-266 96 M RAM	Standard NT 4.0 w/sp 6a. BMC Agent w/Security Patch	Administrator – Sys Admin Perform – PP Administrator JoeUser - User
Artemis 192.168.0.115	Spark 5	Solaris 2.7, BMC Agent w/Security Patch	Administrator – Sys Admin Perform – PP Administrator JoeUser – Unauthorized User

9. Results of the Evaluation

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures. [CCEVS_PUB 3]. The validation team has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology [CEM], and the CCEVS. The validation team therefore concludes that the evaluation and its results of **pass** are complete.

9.1 Assurance Content

The evaluation provides for Assurance at the EAL 2 level with assurance components as shown in the table below:

EAL2 Assurance Requirements

Assurance Class	Assurance Family

Assurance Class	Assurance Family
ST Evaluation	ASE_DES.1
	ASE_ENV.1
	ASE_INT.1
	ASE_OBJ.1
	ASE_PPC.1
	ASE_REQ.1
	ASE_SRE.1
	ASE_TSS.1
Configuration Management	ACM_CAP.2
Delivery and Operation	ADO_DEL.1
	ADO_IGS.1
Development	ADV_FSP.1
	ADV_HLD.1
	ADV_RCR.1
Guidance Documents	AGD_ADM.1
	AGD_USR.1
Tests	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessment	AVA_SOF.1
	AVA_VLA.1

10.Validator Comments/Recommendations

As with any evaluation, this evaluation shows that the evaluated configuration meets the security claims made, with a certain level of assurance. This evaluation did *not* evaluate the networking functions available in the commercial product—these functions are disabled in the evaluated configuration. It is also worth noting that the evaluated configuration is a special configuration that, after purchase, is installed and configured by the vendor at the customer's premises; this evaluation does not apply to the "standard" product that can be purchased and directly installed by customers. This ST only claims that unauthorized users cannot start the collection process (the process that gathers data about the system); it makes no claims that the collection process cannot be stopped, nor does it claim that the TOE protects the generated data. The product has been evaluated at the assurance level of EAL 2 that it meets its functional claims.

The validator observed that the evaluation and all of its activities were in accordance with the CC the CEM, and CCEVS practices; and that the CCTL presented appropriate CEM work units and rationale. The validation team therefore concludes that the evaluation, and its results of **pass,** are complete and correct.

11. Annexes

None, the remainder of this page is blank.

12. Security Target

The Security Target is provided separately; it is Version 1.0, March 15, 2002.

13. List Of Acronymns And Glossary Of Terms

The following acronyms are provided for reference:

CC	Common Criteria
CCEL	Common Criteria Evaluation Laboratory
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CI	Configuration Items
CSC	Computer Sciences Corporation
DSA	Developer Security Analyst
EAL	Evaluation Assurance Level
EDR	Evaluation Discovery Report
ETR	Evaluation Technical Report
MRA	Mutual Recognition Arrangement
NIAP	National Information Assurance Program
NIST	National Institute of Science & Technology
NSA	National Security Agency
OR	Observation Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirements
SOF	Strength of Function
ST	Security Target
TCSEC	Trusted Computer Systems Evaluation Criteria
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface

The following terms are provided for reference:

User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Human user	Any person who interacts with the TOE.
Authorized User	A user that, in accordance with the TOE Security Policy (TSP) may perform an action. (As identified by group membership.)
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Identity	A representation (e.g., a string) uniquely identifying an authorized user, which can be either the full or abbreviated name of that user or a pseudonym.
Authentication data	Information used to verify the claimed identity of a user.
Collection Process	A TOE process that collects pre-defined data for a pre-defined period of time, and results in data that is re-formatted into UDR format for use by the Manager, Predict, Analyze, and Visualizer components of the TOE.

14. Documentation

The evidence used in this evaluation is based solely uponthe product and the following documentation:

[BPP]	BMC Software PATROL® Perform/Predict, Version 6.5.30
[BPP_IND]	BMC Software PATROL® Perform/Predict, Version 6.5.30, Independent Testing
[BPP_TP]	BMC Software PATROL ® Perform/Predict, Version 6.5.30,Vulnerability Assessment: Vulnerability Assessment: Test Plan, Test Cases, Test Report
[BPP_ST]	BMC Software, PATROL ® Perform/Predict, Version 6.5.30, Security Target, Version 1.0
[PP-001a]	BMC 6.5.30 NT and Unix Release Notes (email dated:1/23/01) plus mkPATROL for NT Performance Information for 6.5.30 Release Notes/NT Manager and Secure Nodes, 3/8/2001
[PP-001b]	BMC PATROL for Unix Performance Information for 6.5.30 Release Notes/Unix Manager and Secure Nodes, 3/8/2001
[PP-002a]	BMC PATROL for Microsoft Windows 2000 Servers, Release Notes Version 6.5.30 1/29/01, dated 2/5/2001
[PP-002b]	BMC PATROL RTM for Unix Performance Release Notes, Version6.5.30, 1/29/01, dated 2/5/2001

[PP-003]	BMC PATROL for Unix Performance Getting Started, dated 1/10/2001
[PP-004]	BMC Software Configuration Management Document for Security, dated 6/11/2001
[PP-005]	BMC Product Packaging and Delivery Procedures for PATROL Classic, PATROL Enterprise Manager, and PATROL Perform/Predict, dated 9/7/2001
[PP-006]	BMC Software, PATROL Perform/Predict, Version 6.5.30 Design Document, dated 2/2/2002
[PP-007]	BMC Software, PATROL Perform/Predict, Version 6.5.30 Security Target, dated 1/24/2002
[PP-008]	BMC Security Test Document for Perform/Predict Product Version 6.5.30, dated1/24/2002
[PP-009]	BMC Software, PATROL Perform/Predict, Version 6.5.30 Vulnerability Assessment, dated 1/29//2002
[PP-010]	BMC Authorization Test Cases, dated 3/8/2002
[PP-011]	BMC Technical Bulletin, dated3/8/2002

The evaluation and validation methodology was drawn from the following:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1.
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1.
[CC_PART2A]	Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, version 2.1.
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB 1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0, May 1999.

[CCEVS_PUB 2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000

[CCEVS_PUB 3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 1.0, January 2002.

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, 31 August 2000.