# National Information Assurance Partnership


TM

# Common Criteria Evaluation and Validation Scheme Validation Report

## Tumbleweed MMS ™ and IME ™ Version 5.5.3

**Report Number: CCEVS-VR-05-0105**
**Dated: June 23, 2005**
**Version: 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**

# TABLE OF CONTENTS

# 1 Executive Summary

This report documents the NIAP validator's assessment of the evaluation of the Tumbleweed MMS™ and IME™ Version 5.5.3, a product of Tumbleweed Communications Corp., Redwood City, CA. It presents the evaluation results, their justifications, and the conformance results. 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.

The evaluation was performed by the Arca Common Criteria Testing Laboratory (CCTL), and was completed during June 2005. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Arca CCTL. The evaluation determined that the product is both **Common Criteria Part 2 extended and Part 3 augmented**, and meets the assurance requirements of EAL 2 augmented with ACM_CAP.3: Authorisation Controls, ACM_SCP.1: TOE CM coverage, and ADV_HLD.2: Security enforcing high-level design (hereafter EAL 2+). The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific organizational security policies while countering specific threats.

Tumbleweed MMS™ and IME™ Version 5.5.3 (hereafter Tumbleweed MMS/IME) is an electronic messaging application. The Target of Evaluation (TOE) was evaluated using the *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 2001 [CCV2.1], and the *Common Methodology for Information Technology Security Evaluation*, Version 1.0, Evaluation Methodology, August 1999 [CEMV1.0]. The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4]. The Security Target (ST) for Tumbleweed MMS™/IME™ is contained within the document *Security Target for Tumbleweed MMS™ and IME™ Version 5.5.3,* dated June 1, 2005 [ST]. The ST has been shown to be compliant with the *Specification of Security Targets* requirements found within Annex A of Part 1 of [CCV2.1].

The Tumbleweed MMS/IME is an all-software TOE. It consists of two components that comprise the TOE:

- The Tumbleweed Integrated Messaging Exchange (IME) is an electronic message (email) application that can deliver messages and attached files (hereafter IME packages) to any recipient with an account on the IME server. The IME server is accessed via a Web browser interface and provides status information on when an IME package was sent and received. IME provides several security features from the sender's desktop to the recipient's desktop, including use of encrypted connections (HTTPS via SSL) and password protection of files. Account management may be distributed using a hierarchy of group managers.

- The Tumbleweed Messaging Management System (MMS) is the interface between an organization and Internet email. MMS provides enforcement of filtering policies on email delivered via the Simple Mail Transport Protocol (SMTP). Such policies include filtering based on key word detection, presence of attachments, virus scanning, and S/MIME signatures. The MMS is also capable of maintaining an audit trail of email communication. The Tumbleweed MMS and IME servers may be configured to exchange email (as IME packages) with each other.

Aspects of the following security functions are controlled / provided by the TOE in conjunction with the IT environment:

- Identification and authentication
- Role-based security management
- IME package access control
- Email policy enforcement
- Audit
- Message confidentiality and non-repudiation
- Trusted path between TOE components

The following are explicitly excluded from the TOE configuration, but are included in its environment:

- Hardware platforms and Windows 2000 Operating Systems;
- Database server (Microsoft SQL 2000 Server);
- Web browser (Microsoft Internet Explorer);
- Web server (Microsoft IIS);
- Cryptographic services of the operating system and RSA's Cryto-C product; and
- Network hardware and software (e.g., firewalls and routers)

It is assumed that the environment will counter the threats of unauthorized access to the physical components of the TOE - server and client platforms. It is also assumed that excluded software (e.g. Microsoft Windows 2000 and its services; and firewall software) will operate correctly and securely.

The overall Strength of Function (SOF) claim for the TOE is SOF-basic.

# 2 Identification

**TOE**: Tumbleweed MMS™ and IME™ Version 5.5.3

**Evaluated Software**: Tumbleweed MMS™ and IME™ Version 5.5.3

**Developer**: Tumbleweed Communications Corp.
700 Saginaw Drive
Redwood City, CA 94063

**CCTL**: Arca Common Criteria Testing Laboratory
SAVVIS Communications
45901 Nokes Boulevard
Sterling, VA 20166.

**Validation Team:** Bradford O'Neill (The MITRE Corporation)

**CC Identification**: *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999 [CCV2.1].

**CEM Identification**: *Common Methodology for Information Technology Security Evaluation*, Version 1.0, Evaluation Methodology, August 1999 [CEMV1.0].

**Interpretations**: All NIAP and CCIMB interpretations as of the date of the Kick-off meeting held on October 28, 2002, were considered during the evaluation. The interpretations listed below had a direct impact on the work performed.

.

**Interpretations**

| Interpretation: | Interpretation Description: | Requirements Affected by Interpretation: |
|---|---|---|
| **International Interpretations** | | |
| INTERP-003 | Unique identification of configuration items in the configuration list | ACM_CAP |
| INTERP-004 | ACM_SCP.*.1C requirements unclear | ACM_SCP.1.1D |
| INTERP-065 | No component to call out security function management | FMT_SMF.1 |
| **National Interpretations** | | |

| | | |
|---|---|---|
| NIAP-0375 | Elements Requiring Authentication Mechanism | FIA_UAU.1.2 |
| NIAP-0407 | Empty Selections Or Assignments | FDP_ACF.1.3, FDP_ACF.1.4 |
| NIAP-0410 | Auditing Of Subject Identity For Unsuccessful Logins | FAU_IME_GEN.1.2, FAU_MMS_GEN.1.2, FAU_MMS_GEN.2.1 |

# 3 Security Policy

The Tumbleweed MMS/IME security policy is reflected in the security functional requirements for the TOE described in sections 5.1 and 5.2 of the ST and for the IT environment described in sections 5.3 and 5.4 of the ST. A description of the principle security policies is as follows:

- **Identification and authentication:** The TOE in conjunction with the IT environment requires users to be identified and authenticated before being allowed access to the system. The SMTP messages that are accepted by MMS from external, anonymous users are the only exception. The IME and MMS components support administrative access via a Web browser interface. The IME component supports access to IME packages by non-administrative users. Under the non-repudiation policy, described below, S/MIME encoded SMTP messages that have been digitally signed may be detected and verified by the MMS component working in conjunction with the IT environment.

- **User access control:** The TOE enforces an access control policy for non-administrative IME users. The access control policy ensures that each user is only allowed to view and manage the IME packages and folders associated with his account. Table 2 in the ST provides details about the access control policy.

- **Email policy enforcement.** The MMS component permits the administrator to define an email policy that is applied against incoming and outgoing email messages. The policy is a set of rules that describe the matching criteria and the actions to be taken when a match occurs. MMS rules support the following actions: delivery to IME (redirect), normal delivery, deferred delivery, return to sender, drop, detain, and quarantine. The following matching criteria categories are supported: basic word list lookup, attachment detection, virus detection, and detection of S/MIME signatures (security). To support the virus detection, the TOE supports automatic downloading of the most recent virus definition file on a periodic basis.

- **Role-based security management:** The TOE supports four administrative roles. In addition to an administrator role with full control, the IME component supports a group manager role that is limited to managing user accounts associated with a

particular group of IME mail accounts. The MMS component supports two roles: a 2nd level administrator with full control and a 1st level administrator role with full operational control but which is restricted from modifying the administrator accounts and audit logging parameters. Table 3a in the ST provides additional details.

- **Audit:** The TOE in conjunction with the IT environment provides an auditing capability. Auditable events for the IME and MMS components are identified in tables 4 and 8 of the ST.

The TOE also provides support for other significant objectives (see section 3.3 of the ST):

- **Confidentiality:** The TOE in conjunction with the IT environment ensures that non-administrative users access IME component via HTTPS (SSL). SSL provides encryption of user data transported over the network.
- **Non-repudiation and message integrity:** The MMS component supports policy rules for detection and verification of digital signatures provided in S/MIME formatted messages sent via SMTP. The actual verification is performed by the RSA Crypto-C module in the IT environment and the TOE is notified if the signature is invalid. The proof of receipt objective is supported by the IME component's capability to track the delivery status for each of an IME package's recipients.
- **Trusted path:** The data transported over network connections between the MMS and IME components are encrypted using SSL. The SSL connections are configured to verify each other's X509 digital certificate.

The security functional requirements for the TOE and the IT environment are documented in section 5 of the ST. A combination of requirements drawn from part 2 of the CC [CCV1.1] and explicitly stated security requirements were necessary due to different levels of reliance of the IME and MMS components on the IT environment. In particular, the IME component's auditing function relies on the Microsoft's Windows 2000 Event subsystem and the MMS component's I&A function relies on Microsoft's SQL 2000's I&A function. As a result, the wording of many explicitly stated security requirements were directly derived from their part 2 counter part and then restricted to either the MMS or the IME component. A summary of the SFRs for the TOE and IT environment are included in the tables below.

**TOE Security Functional Requirements**

| **Class FAU: Security Audit** | |
|---|---|
| FAU_SAR.1 | Audit review |
| FAU_IME_GEN.2 | Audit data generation |
| FAU_MMS_ARC.1 | Archival of triggered policy violations |

| | |
|---|---|
| FAU_IME_SAR.2 | Restricted audit review |
| FAU_MMS_SAR.3 | Selective audit |
| FAU_MMS_STG.3 | Action in case of possible audit data loss |
| **Class FCO: Communication** | |
| FCO_IME_NRR.1 | Selective proof of receipt |
| FCO_MMS_NRV.1 | Non-repudiation verification of origin |
| **Class FDP: User Data Protection** | |
| FDP_ACC.1 | Subset access control |
| FDP_ACF.1 | Security attribute based access control |
| FDP_MMS_POL.1 | Policy engine |
| FDP_IME_UCT.1 | Basic data exchange confidentiality |
| **Class FIA: Identification and Authentication** | |
| FIA_UAU.7 | Protected authentication feedback |
| FIA_IME_AFL.1 | Authentication failure handling |
| FIA_IME_SOS.1 | TSF verification of secrets |
| FIA_IME_UAU.1 | Timing of authentication |
| FIA_IME_UID.1 | User identification before any action |
| FIA_MMS_TOA.1 | External user authentication before any action |
| **Class FMT: Security Management** | |
| FMT_MOF.1 | Management of security functions behavior |
| FMT_MSA.1 | Management of security attributes |
| FMT_IME_MSA.3 | Static attribute initialization |
| FMT_MTD.1 | Management of the TSF data |
| FMT_IME_REV.1 | Revocation |
| FMT_SMF.1 | Specification of management functions |
| FMT_IME_SMR.1 | Security roles |
| FMT_MMS_DNL.1 | Virus definition download |
| **Class FPT: Protection of the TSF** | |
| FPT_ITC.1 | Inter-TSF confidentiality during transmission |
| **Class FTA: TOE Access** | |
| FTA_SSL_EXP.1 | TSF-initiated termination |
| **Class FTP: Trusted Path** | |
| FTP.ITC.1 | Inter-TSF trusted channel |

**IT Environment Security Functional Requirements**

| | |
|---|---|
| **Class FAU: Security Audit** | |
| FAU_STG.1 | Protected audit trail storage |
| FAU_MMS_GEN.1 | Audit data generation |
| FAU_MMS_GEN.2 | User identity association |
| FAU_IME_SAR.3 | Selective audit |
| FAU_IME_STG.3 | Action in case of possible audit data loss |
| **Class FCS: Cryptographic Operation** | |
| FCS_CKM.1 | Cryptographic key generation |
| FCO_COP.1 | Cryptographic operation |

| | |
|---|---|
| FCO_MMS_CKM.2 | Cryptographic key distribution |
| FCO_MMS_CKM.4 | Cryptographic key destruction |
| **Class FIA: Identification and Authentication** | |
| FIA_MMS_AUT.1 | Database authentication |
| **Class FMT: Security Management** | |
| FMT_MSA.2 | Protected authentication feedback |
| FMT_MMS_SMR.1 | Secure security attributes |
| **Class FPT: TOE Protection** | |
| FPT_STM.1 | Reliable time stamp |

# 4 Assumptions and Clarification of Scope

## *4.1 Usage Assumptions*

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements.

ADO_DEL.1 Delivery procedures
ADO_IGS.1 Installation, generation, and start-up procedures
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

## *4.2 Environmental Assumptions*

The environmental assumptions listed in the following table are required to ensure the security of the TOE.

**Environmental Assumptions**

| Assumption | Description |
|---|---|
| **A.Admin** | It is assumed that one or more authorized administrators are assigned who are competent to manage the SQL 2000 Database Servers for MMS and IME, the Internal and External HTTP Gateways, the IIS 5.0 web server for MMS, and the Windows 2000 operating systems of MMS and IME, who are competent to manage the security of the information these systems contain, and who can be trusted not to deliberately abuse their privileges so as to undermine security. |
| **A.Locate** | The processing resources of the TOE are assumed to be located within controlled access facilities which will restrict unauthorized physical access. |
| **A.Message_Secure** | The IME user will select the proper security protections for messages (e.g. encrypt, plaintext). |

| Assumption | Description |
|---|---|
| | |
| **A.Timestamp** | A reliable source of time is provided by the Windows 2000 operating system for MMS, IME, and the two HTTP Gateways communicating with IME. |
| **A.User_Auth_Credentials** | The user will not disclose their password. |

### *4.3 Clarification of Scope*

Tumbleweed MMS/IME administrator and user guides describe several significant capabilities that were not included in the ST and were outside the scope of the evaluation. The MMS policy enforcement support for "SPN" (for Secure Public Network) and "Headers" policy types was not included in the FDP_MSS_POL SFR and was not verified by testing. Also, the IME capability to automatically activate disable, and delete accounts was not claimed in the ST. The IME is capable of sending packages via SMTP to email recipients that do not have an account on the IME server. Only the "Secure Envelope" method of delivery via SMTP is included in the scope of the evaluation. Package delivery via SMTP using temporary accounts or automatic recipient enrollment was not claimed in the ST and was not evaluated. "Secure Envelope" packages are encrypted using a password specified by the sender. When the Secure Envelope package is delivered to the recipient, the recipient must authenticate to the Secure Envelope package using the package's password. This authentication occurs outside the TOE and no assurance or SOF is claimed for this mechanism. The TOE claims that it can securely create the packages but cannot assure actions outside the TOE boundary.

Tumbleweed MMS/IME is intended to be used as a set of components in an electronic messaging application. There are other components in the IT environment required to securely handle messages. The TOE relies upon services in the IT environment to perform some of its security functions. Namely, the following products are required to be in the IT Environment:

- Intel Pentium computers for servers and gateways
- Operating system (Microsoft's Windows 2000 Server with SP4)
- Database server (Microsoft's SQL 2000 with SP3)
- Web Server (Microsoft's IIS 5.0)
- Cryptographic services (RSA's Crypto-C, version 5.2.1)
- Web Client (Microsoft Internet Explorer 6.0 with SP1)

These products are not within the scope of the TOE.

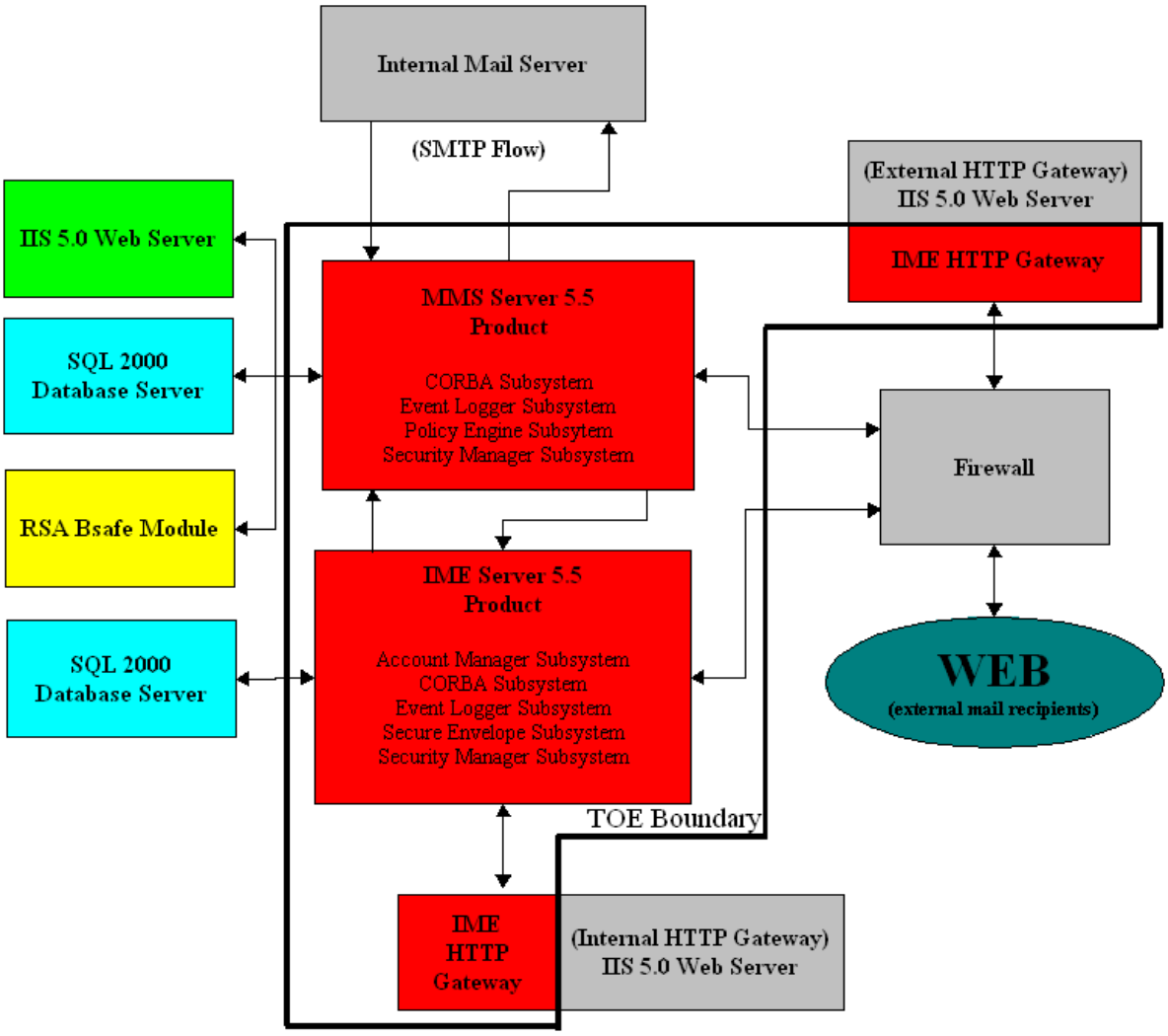
The evaluation of this TOE is not directly tied to possible evaluations of any of those other components in an electronic messaging application. In particular, the evaluation of

this TOE does not imply that all of the properties required of the Tumbleweed MMS/IME for the evaluation of those other products have been included in this evaluation. This is not necessarily a limitation upon the capabilities of this product or those other components of the messaging environment, but rather it is a statement of the limitations on the scope of the analysis that was performed for this evaluation.

# 5 Architectural Information

The Tumbleweed MMS/IME TOE is an electronic messaging application that consists of the IME and MMS server components. The IME component also includes an HTTP Gateway subcomponent that may be installed on separate processor. The evaluated configuration of the TOE consists of two IME HTTP Gateways for internal and external users respectively, as depicted in the following figure. The MMS server accepts email via SMTP. The IME server's interface for non-administrative users is via a Web browser. The administrative interface for both servers is via a Web browser. The hardware for the servers and gateways is an Intel Pentium based processor with the processors inter-connected with a TCP/IP network. The hardware and network components are outside the TOE boundary.

**An architectural diagram of the TOE.**




# 6 Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

- Tumbleweed MMS ™ and IME ™ Version 5.5.3 Security Target
- Tumbleweed IME Server for Windows Administrator's Guide, Release 5.5 Reference AG-S-WIN-550G-Rev00
- Tumbleweed MMS Administrator's Guide Release 5.5 AG-MMS-550-Rev00
- Tumbleweed IME ™ Version 5.5 (Build: 4018) online central help

- Tumbleweed Secure Redirect Administrator's Guide, Release 5.5 Reference AG-MMS-550-Rev00
- Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed MMS ™ and IME ™ Version 5.5.3, version 2.1, dated June 1, 2005

# 7 IT Product Testing

## *7.1 Developer Testing*

The vendor testing covered all of the security functions identified in Section 6.1 of the ST. These security functions were: Audit, Identification and Authentication, Message Security, Role-Based Access, Role Management, and Audit. At EAL2, vendor testing must demonstrate correspondence between the tests and the functional specification. However complete testing is not required; "coverage analysis need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested."[1]

The testing was focused on demonstrating that the SFRs worked as claimed in the ST. The test procedures consisted primarily of manually invoking functions described in the product's user and administrative guides and verifying the function's behavior. In general, only those user interface functions that were directly related to SFRs were explicitly verified. The testing of the MMS policy enforcement capabilities (i.e., related to the FDP_MMS_POL.1, FCO_MMS_NRV.1, and FMT_MSS_DNL.1 SFRs) was more involved and involved three steps: 1) creating a policy via the MMS administrator user interface, 2) sending an message to the MMS server's SMTP port, and 3) verification that the appropriate action had taken place (e.g., mail delivered to the recipient's IME inbox). The testing verified that the policy categories (i.e., Basic, Attachment, Virus, and Security) and actions (i.e., Drop, Return to sender, Quarantine, Detain, Redirect, Defer deliver, and Delivery normally) worked as claimed. The testing was performed at a high level using a representative sub function from each policy type. As a result, the testing explicitly verified only a small portion of the MMS extensive policy enforcement capabilities (e.g., testing did not include word list matching within the files types listed in appendix A or using regular expressions described in appendix B). The following MMS policy sub functions were explicitly tested:

- Basic: detection of keyword in subject line
- Attachment: detection of the existence of an attachment
- Security: validate S/MIME signature using RSA's Crypto C component
- Virus: detection of the Back Oriface virus

[1] CEM, V1.0, paragraph 6.8.2.2 (application note for EAL2:ATE_COV.1)

The evaluator determined that the vendor tested (at a high level) most of the security-relevant aspects of the product that were claimed in the ST. The evaluator determined that the developer's tests were sound in their approach. The test document provided the configuration of the test hardware and software, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests. The evaluators determined that the developer's approach to testing the TSFs was appropriate for this EAL2 evaluation.

### *7.2 Evaluator Independent Testing*

At EAL 2, the stated purpose of the evaluator's independent testing activity "is to determine, by independently testing a subset of the TSF, whether the TOE behaves as specified, and to gain confidence in the developer's test results by performing a sample of the developer's tests." (CEM 6.8.4.1). The CEM further instructs the evaluator to consider a number of factors including: the "Rigour of developer testing of the security functions. Some security functions identified in the functional specification may have had little or no developer test evidence attributed to them." (CEM 6.8.4.3.2) As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

The evaluation team verified that the TOE was installed as is specified in the secure installation procedures, reran a representative sample (roughly 35%) of the developer tests and verified the results. The evaluation team then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

The test environment for the TOE resembled a representative environment for an electronic message mail application, with the exception that the TOE was not connected directly to the public Internet during testing. Instead, the environment provided attacking machines to simulate the hostile environment of the public Internet, internal and external gateways, an external client host, and a mail/DNS/client server to create and send mail messages, provide name service functionality, and the Web browser administrative connections to the IME and MMS servers. The installation of the TOE was done in accordance with the product's Administrator and Installation guides which specifies the configuration of Microsoft's Windows 2000. The installation guide lists the security critical patches with which the MMS and IME components are compatible and contains explicit instructions not to install any additional security critical patches that are recommended by Microsoft's Windows Update capability. At the time of product testing additional security critical patches were available that were not in this list and, as a result, the test environment was not free of obvious vulnerabilities.

Test results, which are contained in proprietary reports, were satisfactory to both the Evaluation Team and the Validation Team.

### *7.3 Strength of Function*

The TOE depends on the strength of the passwords used to access the IME and MMS servers. For this mechanism a qualification of its security behavior was made using the results of a quantitative or statistical analysis of the security behavior of the mechanism and the effort required to overcome the mechanism. A strength-of-function (SOF) claim of SOF-basic was made for accounts on the IME server. The basis of the claim of SOF-basic is the enforcement of the policy that passwords must contain a minimum of 8 characters with at least 1 numeric character and 1 alphabetic character and that account access is locked out after 10 failed attempts. The SOF analysis used these password requirements to justify a ranking of SOF-basic which effectively requires resistance to password guessing attacks of greater than one day. No SOF claim is made in relation to the package passwords or for administrator accounts on the MMS Server because the authentication mechanism is primarily enforced by the IT environment.

### *7.4 Vulnerability Analysis*

The vendor searched for publicly known vulnerabilities specifically related to the TOE, as well as publicly known vulnerabilities in the third-party products that are incorporated in the TOE. No publicly-known vulnerabilities specific to the evaluated version of Tumbleweed MMS/IME were found. The known vulnerabilities in the third party products were examined, and were either countered or shown to be unlikely to be exploitable in the intended environment. The following public domain sources were used to identify and search for relevant vulnerabilities:

- Carnegie Mellon CERT Coordination Center (www.cert.org)
- CERIAS Cassandra (cassandra.cerias.purdue.edu)
- Common Vulnerabilities and Exposures (www.cve.mitre.org)
- ICAT Metabase (icat.nist.gov)
- SecurityFocus Vulnerability Database (www.securityfocus.com)
- SysAdmin, Audit, Network, Security Institute (www.sans.org)

The Tumbleweed MMS/IME product is bundled with three significant third party components that are not directly maintained by Tumbleweed. Publicly available patches to or newer versions of these components that might mitigate obvious vulnerabilities cannot be installed independently by the end-users of Tumbleweed MMS/IME. The first two components are included in the TOE and a search of obvious vulnerabilities related to their functions was performed as part of the AVA_VLA.1 work units. The Crypto-C component was relegated to the IT environment and a search for obvious vulnerabilities related to its functions was outside the scope of the evaluation.

- OmniORB version 4.0
- OpenSSL, version 0.9.6k
- RSA Crypto-C version 5.2.1

The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product. The specific threats that the TOE is designed to counter are listed in section 3.2.1 of the ST.

# 8 Evaluated Configuration

The evaluated version of the Tumbleweed MMS/IME product is version 5.5.3. Tumbleweed provides delivery of the MMS and IME components through electronic deliveries. The names of the files containing the TOE are as follows:

- IME5_5Installer.zip: Installer for the IME product.
- IME55P3_Windows.zip: Installer for the patch to the IME product.
- MMS_55P3_4039.exe: Installer for the MMS product
- MMS_55P3_HF3.exe: Installer for Hotfix 3 of the MMS product.
- MMS55P3_HF4.zip: Installer for Hotfix 4 of the MMS product.

# 9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC, Version 2.1; CEM, Version 1.0, and all applicable NIAP CCEVS and International Interpretations in effect on October 28, 2002.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component and for the augmented assurance components: ACM_CAP.3, ACM_SCP.1, and ADV_HLD.2. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The evaluation determined that the product is both **Common Criteria Part 2 extended and Part 3 augmented**, and meets the assurance requirements of EAL 2 augmented by ACM_CAP.3, ACM_SCP.1, and ADV_HLD.2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by Arca CCTL. The security assurance requirements are displayed in the following table.

**TOE Security Assurance Requirements**

| Assurance Component ID | Assurance Component Name |
|---|---|
| ACM_CAP.3 | Authorisation Controls |

| | |
|---|---|
| ACM_SCP.1 | TOE CM coverage |
| ADO_DEL.1 | Delivery procedures |
| ADO_IGS.1 | Installation, generation, and start-up procedures |
| ADV_FSP.1 | Informal functional specification |
| ADV_HLD.2 | Security enforcing high-level design |
| ADV_RCR.1 | Informal correspondence demonstration |
| AGD_ADM.1 | Administrator guidance |
| AGD_USR.1 | User guidance |
| ATE_COV.1 | Evidence of coverage |
| ATE_FUN.1 | Functional testing |
| ATE_IND.2 | Independent testing – sample |
| AVA_SOF.1 | Strength of TOE security function evaluation |
| AVA_VLA.1 | Developer vulnerability analysis |

The Validation Team agreed with the conclusion of the Arca CCTL Evaluation Team, and recommended to CCEVS Management that an EAL2 augmented (with ACM_CAP.3, ACM_SCP.1, and ADV_HLD.2) certificate rating be issued for Tumbleweed MMS/IME.

# 10 Validator Comments/Recommendations

## *10.1 Reference Mediation and Domain Separation SFRs not included*

The customary TOE protection security functional requirements (i.e., FPT_SEP.1 "TSF Domain Separation" and FPT_RVM.1 "Non-bypassability of the TSP") have not been included for the TOE or its IT environment. For the Tumbleweed MMS/IME evaluation, the FPT_SEP.1 and FPT_RVM.1 SFRs were not needed to address the specific threats and organizational security policies listed in the ST. When these TOE protection SFRs are not included in the ST, the evaluators are instructed to omit several activities involving searches for ways of bypassing the TOE's security policies (e.g., ADV_FSP in CEM 6.6.2 and ADV_VLA in CEM 6.9.2.2).

# 11 Security Target

The Security Target for Tumbleweed MMS/IME is contained within the document *Security Target for Tumbleweed MMS™ and IME™ Version 5.5.3* dated June 1, 2005. [ST]. The ST is compliant with the *Specification of Security Targets* requirements found within Annex A of Part 1 of the CC [CCV2.1].

# 12 Glossary

The following table is a glossary of terms used within this validation report.

| Acronym | Expansion |
|---|---|
| CC | *Common Criteria for Information Technology Security Evaluation*. [Note: Within this Validation Report, CC always means Version 2.1, dated August 1999.] |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CCTL | Common Criteria Testing Laboratory |
| CCIMB | Common Criteria Interpretations Management Board |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| GUI | Graphical User Interface |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| I&A | Identification and Authentication |
| IME | Integrated Messaging Exchange |
| IP | Internet Protocol |
| IT | Information Technology |
| MMS | Messaging Management System |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NVLAP | National Voluntary Laboratory Accreditation Program |
| PP | Protection Profile |
| SFR | Security Function Requirement |
| S/MIME | Secure / Multipurpose Internet Mail Extensions |
| SMTP | Simple Mail Transport Protocol |
| SOF | Strength of Function |
| SSL | Secure Sockets Layer |
| ST | Security Target |
| TCP | Transmission Control Protocol |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |

# 13 Bibliography

***URLs***

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap.nist.gov/cc-scheme).
- Arca CCTL, SAVVIS Solutions (http://www.savvis.com).
- Tumbleweed Corporation (http://www.tumbleweed.com).

***CCEVS Documents***

[CCV2.1] *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999.

[CEMV1.0] *Common Methodology for Information Technology Security Evaluation*, Version 1.0, Part 2: Evaluation Methodology, August 1999.

[CCEVS3] *Guidance to Validators of IT Security Evaluations*, Version 1.0, February 2000.

[CCEVS4] *Guidance to Common Criteria Testing Laboratories*, Draft, Version 1.0, March 2000.

***Other Documents***

[ST] *Security Target for Tumbleweed MMS™ and IME™ Version 5.5.3,* Version 4.5, June 1, 2005