ASSURANCE CONTINUITY MAINTENANCE REPORT FOR ForeScout CounterACT v7.0.0 with Hotfix v1.2

Maintenance Report Number: CCEVS-ACMR-VID10342-0006

Date of Activity: 13 March 2013

References: Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation", 8 September 2008;
Common Criteria Assurance Maintenance Impact Analysis Report (IAR) ForeScout CounterACT v7.0.0 with Hotfix v1.2

Documentation Updated:

Assurance Family	Title	Version	Date
ASE	ForeScout Technologies, Inc. CounterACT v7.0.0 with Hotfix v1.2 Security Target	2.2	02/18/2013
ALC	ForeScout Technologies, Inc. CounterACT v7.0.0 with Hotfix v1.2 Configuration Management Document	0.8	02/18/2013
ATE	ForeScout Technologies, Inc. CounterACT v7.0.0 with Hotfix v1.2 (cc-test-700.docx)	N/A	01/24/2013
AGD	ForeScout Technologies, Inc. CounterACT v7.0.0 with Hotfix v1.2 Common Criteria Supplement to the Administrative Guidance	1.2	02/18/2013
AGD	ForeScout Technologies, Inc. ForeScout CounterACT Version 7.0.0 Release Notes	7.0.0	07/2012

Assurance Continuity Maintenance Report

The Corsec Security, Inc., acting for ForeScout technologies, Inc. the vendor of ForeScout CounterACT v7.0.0 with Hotfix v1.2, submitted an Impact Analysis Report (IAR) to CCEVS for approval in February 2013. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation", 8 September 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes, and the security impact of the changes.

Changes to TOE:

- Total Changes included in IAR – 29;
- Changes with major security relevance – 0;
- Changes with minor security relevance – 11; and

- Changes with no security relevance – 18.

Types of Changes:

- System Changes (4) – modifications allowing greater numbers of machines to be processed, supporting extensions to network protocol suites, accommodate underlying OS upgrades, and supporting external logging services;
- Display Changes (4) - modifications to how TOE data is organized and displayed;
- Functional Changes (17) – miscellaneous changes to the functional operation of the TOE that did not alter security operation or introduce any new interfaces; and
- Not Applicable (4) - changes where modifications were made to TOE components/functions that were outside claimed TOE functionality and were not included in the original evaluation.

TOE Changes with Security Significance

Of the 29 changes made to the TOE 11 were described as having minor security significance. None of these changes required changes to the Security Target.

They are each covered below.

Change Title	Affected SFRs	Change Description	CCEVS Assessment
Enhanced Groups Control	FMT_MTD.1 FMT_SMF.1 FDP_ACC.1-1 FDP_ACF.1-1 FMT_MSA.1-1	This feature enhances the CounterACT Groups feature that was available in the evaluated version. Provides improved displays for users with access to groups and which hosts are in the groups had been added.	This allows administrators a new way to view information already maintained by the TOE. Agree with the minor security impact.
Login to CounterACT via User Groups	FMT_MTD.1 FMT_SMF.1	User creation is streamlined by defining CounterACT user groups based on existing Active Directory and RADIUS7 user groups.	This provides an accelerated way for administrators to perform an existing function using existing attributes. Agree with the minor security impact.
Large-Scale Reports Management	FAU_SAR.1 FMT_MTD.1	The Reports Plugin has been upgraded with several tools that facilitate management of multiple reports in a large-scale deployment scenario.	This provides additional access to existing features and information. Multiple existing operations can now be run simultaneously.

			Agree with the minor security impact.
MAC Based Access Control	FDP_ACC.1-1 FDP_ACF.1-1 FMT_MSA.1-1	Hosts can now be detected, managed, and controlled via the host MAC address.	MAC address is an existing security attribute. This provides a new way to use existing security information. Agree with the minor security impact.
Inherited Policy Recheck	FMT_MSA.1-1	CounterACT can now be instructed to automatically apply main rule recheck definitions to all sub-policies, rather than defining the recheck value for each sub-rule.	This change makes existing capabilities easier and more flexible to use. Information can be grouped together rather than having to be processed on an individual basis. Agree with the minor security impact.
Fine-Tuned Authentication Login Detection	FMT_MSA.1-1 FMT_SMF.1	A user can now search for hosts that logged into the network by the protocol or server IP address used to login.	This change allows access to existing information and makes capabilities easier to use. Agree with the minor security impact.
Extended Support for SNMP	FMT_MSA.1-1 FMT_MTD.1	Extended support for SNMP allows extended visibility for third-party integration.	Support is provided for enhanced versions of SNMP. Agree with the minor security impact.
Syslog Event Filtering Enhancements	FAU_GEN.1 FAU_STG.1	Appliance Operating System Syslog events can now be sent to a Syslog server.	Syslog exists in the environment. Existing TOE functions are not affected. Agree with the minor security impact.

New Actions for Modifying Policies	FDP_ACF.1-1 FMT_MSA.1-1	Several new actions for modifying policies have been included, such as Delete Properties, Delete Host, and Recheck Host.	Change allows operations that had to be executed singularly to be combined. It provides flexibility to existing capabilities. Agree with the minor security impact.
Improved Log Reporting on Policy Actions	FAU_GEN.1	Policy audit logs now provide more information. Additionally, action tooltips have been improved.	This change allows additional detail to be displayed. Agree with the minor security impact.
Vulnerability Scanning Wizard Removed	SSC_ACT_EXT.1 SSC_ANL_EXT.1 SSC_SCN_EXT.1	The Vulnerability Scanning Wizard has been retired, and the functionality moved to the *Microsoft Vulnerabilities* property and *Open Ports* property.	Access to existing information has been changed, the same functions are provided. Agree with the minor security impact.

CCEVS concluded none of the changes included in the IAR had greater security impact than was reported. All changes have either minor or no security impact. No new security features are added and no Security Functional Requirements needed to be changed on account of the changes included in the IAR. No major changes were required in the ST.

Conclusion

CCEVS considers the original assurance has been maintained for the above-cited version of the product.