Record ID: VID10349-0001-ACMR

CCEVS Approved Assurance Continuity Maintenance Report

Product:	Cisco Nexus 7000 Series Switch running NX-OS version 5.1(1a) and Cisco Secure Access Control Server (ACS) running ACS version 5.2 patch 3
EAL:	4 + ALC_FLR.2
Date of Activity:	28 January 2013
References:	CCIMB-2004-02-009 Assurance Continuity: CCRA Requirements, Version 1.0, February 2004 Impact Analysis Report for Common Criteria Assurance Maintenance Update of Cisco Nexus 7000 Series Switch running NX-OS version 5.1(1a) and Cisco Secure Access Control Server (ACS) running ACS version 5.2 patch 3 to Cisco Nexus 7000 Series Switch running NX-OS version 5.2(5) and Cisco Secure Access Control Server (ACS) running ACS version 5.2 patch 10, August 2012. Impact Analysis Report for Common Criteria Assurance Maintenance Update of Cisco Nexus 7000 Series Switch running NX-OS version 5.1(1a) and Cisco Secure Access Control Server (ACS) running ACS version 5.2 patch 3 to Cisco Nexus 7000 Series Switch running NX-OS version 5.2(5) and Cisco Secure Access Control Server (ACS) running ACS version 5.2 patch 11, November 2012.
Documentation Updated:	Nexus 7000 Series Switch Security Target Version 0.22 dated April 2011 Configuration Management, Lifecycle and Delivery Procedures for Cisco Nexus 7000 Series Switch and Cisco Secure Access Control Server (ACS), Document Version 1.2, February 2011 Nexus 7000 Series Switch Operational User Guidance (Common Criteria Specific), Version 0.5, February 2011 Cisco Nexus 7000 Series Switch Preparative Procedures Wrapper, Version 0.6, February 2011 Nexus 7000 + ACS Common Criteria Test Documentation, version 1.4, 2/10/2011

I. Introduction

In August 2012, Cisco submitted an Impact Analysis Report (IAR) to CCEVS for approval. The IAR is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version 1.0, February 2004. 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. In addition, an updated IAR was subsequently delivered in November 2012.

II. Changes to the TOE

The changes implemented by the developer include patches and bug fixes to the software and documentation fixes to the ST, and operations manuals. The following tables summarizes these changes.

Evidence Affected

Table 1: Affected Developer Evidence

Assurance Family	Title
ASE	Nexus 7000 Series Switch Security Target Version 0.22 dated, April 2011
ACM_CAP ACM_SCP	Configuration Management, Lifecycle and Delivery Procedures for Cisco Nexus 7000 Series Switch and Cisco Secure Access Control Server (ACS), Document Version 1.2, February 2011
AGD_OPE	Nexus 7000 Series Switch Operational User Guidance (Common Criteria Specific), Version 0.5, February 2011
AGD_PRE	Cisco Nexus 7000 Series Switch Preparative Procedures Wrapper, Version 0.6, February 2011
AVA_VLA	N/A
ATE	Nexus 7000 + ACS Common Criteria Test Documentation, version 1.4, 2/10/2011

Supporting Analysis

Table 2: Supporting Analysis for Determination of Affected Developer Evidence

Analysis	Determination
a. Has it affected the Security Target?	Yes
b. Has it affected the reference for the TOE (if the assurance baseline includes a component from the ACM_CAP family)?	Yes
c. Has it affected the list of configuration items for the TOE (if the assurance baseline includes a component from the ACM_SCP family)?	Yes
d. Has it affected any of the TSF abstraction levels, that is, the functional specification, the high level design, the low level design or the implementation representation (if the assurance baseline includes a component from the ADV class)?	No
e. Has it affected the architectural description (if the assurance baseline	No

Analysis		Determination
	includes a component from the ADV_INT family)?	
f.	Has it affected the analysis of correspondence (if the assurance baseline includes a component from the ADV_RCR family)?	No
g.	Has it affected the TSP model (if the assurance baseline includes a component from the ADV_SPM family)?	No
h.	Has it affected the guidance documentation (if the assurance baseline includes a component from the AGD class)?	Yes
i.	Has it affected the testing documentation, that is, the analysis of test coverage, the analysis of the depth of testing or the test documentation (if the assurance baseline includes a component from the ATE class)?	Yes
j.	Has it affected the covert channel analysis, the analysis of guidance documentation, the vulnerability analysis (if the assurance baseline includes a component from the AVA class)?	Yes

Table 3: Minor Changes with no Security Relevance

Change Description	# of Bug fixes	Part of TOE?
Minor Changes Non-Security Relevant Commands	435	No
Grammar, Help and Documentation Updates	109	No
Minor Changes for Memory Leaks	532	No
Minor Changes for Telnet and SNMP Management	33	No
Minor Changes for Virtual Private Networks	21	No
Non-security Relevant Hardware	7	No
Minor Changes to Non-security Relevant Firmware	14	No
Minor changes to Switching and Routing Protocols	1176	No
Minor changes for Failover	320	No
Minor Changes to System Load Testing	80	No
Minor Changes to Upgrading Images	508	No
Minor Changes to Licensing	15	No
Minor Changes to Compiler Tools	8	No
Minor Changes to Software outside the TSF Boundary	35	No

ACS Bug Fixes

The following contains the information for the ACS Bug Fixes and rationale as to why they do not affect the TSC:

Table 4: Minor ACS Changes with Rationale for Non-Relevance

Identifier	Component	Headline	Rationale
CSCsz74681	distributed-mgmt	Distribution Management MGM REPLICATION Execute failed	High availability is not relevant to the TSF.
CSCte39351	accessibility	ACS appliance snmp agent process daemon stops	Management using SNMP was outside the scope of the TSF.
CSCtg51846	gui-fw-mgmt	Enum values are not shown in compound conditions in rule	Thresholds and load testing are not security relevant.
CSCth12406	general	ACS 5 does not have option to disable local account on failed attempts	No claims with respect to automatic account disablement were made in the Security Target.
CSCth66302	logging-mgmt	Radius Authentication Request Rejected due to critical logging Error	Thresholds and load testing are not security relevant.
CSCtk96981	import-export	FATAL errors when importing Network Devices using the CLI	Affects a command that is not security relevant.
CSCtl75467	gui-fw-mgmt	ACS5.2 High CPU usage due to failure in startup of adclient.	Thresholds and load testing are not security relevant.
CSCto52051	install	5.2P4 - Patch removal is not working fine	Applies only to a version of software post the evaluated version.
CSCto62265	import-export	Unable to add users,ad,ldap manually while importing clients in CLI	There are no claims about the ability to make changes to the database simultaneously.
CSCto73865	logging-general	Getting exception on Runtime & management logs - Account disablement	No claims with respect to automatic account disablement were made in the Security Target.
CSCto79793	cli-acs	Not able to login to GUI, after acsbackup5.1 and acsrestore 5.2 patch4	Applies only to a version of software post the evaluated version.
CSCto88134	upgrade	Temporary table was missing in 5.2 db after restoring 5.1 backup	Takes the TOE back out of the evaluated version.
CSCto95888	cli-acs	sh acs-logs details cmd does not display	Affects a command that is not security relevant.

		localstore log file name .	
CSCtr78143	gui-fw-mgmt	Multiple Cross--Site Request Forgery and stored XSS in ACS 5.2	Fixes a security vulnerability, but the forms themselves did not affect the TSF.
CSCtr78192	gui-fw-mgmt	Multiple vulnerabilities in the Cisco ACS 5 web interface.	Fixes a security vulnerability, but the forms themselves did not affect the TSF.
CSCts85741	gui-fw-mgmt	Possible SQL Injection point in ACS 5.2	Fixes a security vulnerability, but the forms themselves did not affect the TSF.
CSCtt14745	gui-app	Cannot add group to LDAP identity store.	LDAP functionality was not within the TSF.
CSCtt17019	active-directory	ACS5.x-Issue retrieving additional AD groups when referenced in rules	AD functionality was not within the TSF.
CSCtt21122	import-export	Cannot import command sets with slash '/' in argument	Affects a command that is not security relevant.
CSCtu04594	gui-app	ACS 5.2.0.26.7 - only 50 NDGs shown on GUI with more than 100 configured	Thresholds and load testing are not security relevant.
CSCtu06690	gui-app	ACS network device display filter broken big time	Affects a command that is not security relevant.
CSCtu36357	general	ACS 5 cannot duplicate user account	Affects a command that is not security relevant.
CSCtu89783	radius-token-rt	ACS 5 password expiration policy triggered for token user	RADIUS tokens were not part of the TSF.
CSCtw56498	tacacs-auth	TACACS+ "enable" request is dropped on unknown authen_type	ACS was not used for authorization control in the TSF.
CSCtw64212	cli-acs	'view-logprocessor' Process stuck in 'not monitored'	Affects a command that is not security relevant.
CSCtx19470	general	ACS5 runtime error while try GUI login but all processes are running	High availability is not relevant to the TSF.
CSCtx52048	gui-app	Alignment not proper for certain attr in Internal users/hosts page	Affects a command that is not security relevant.

CSCuc65634	ldap	Cisco Secure ACS TACACS+ Authentication Bypass Vulnerability	LDAP functionality was not within the TSF.
CSCuc87476	ldap	User Authentication with empty password against LDAP store should fail	LDAP functionality was not within the TSF.
CSCuc96058	ldap	LDAP Auth for Anonymous Access Test connection failed in ACS 5.2 pat 11	LDAP functionality was not within the TSF.

Security Relavant Bug Fixes

The following table summarizes the bug fixes with some security relevance by component:

Table 5: Minor Security Relevant Changes

Component	# of fixes	Security Relevance level
CTS	11	Minor
Data Plane Flow Control	32	Minor
Virtualization and Availability	56	Minor
Data Plane Flow Accountability	4	Minor
Secure Management	4	Minor

Table 6: Updated Developer Evidence

Assurance Family	Title	Version	Date
ASE	Cisco Systems Nexus 7000 Series Switch Security Target	0.24	November 2012
ALC_DVS ALC_CMC	Configuration Management, Lifecycle and Delivery Procedures for Cisco Nexus 7000 Series Switch and Cisco Secure Access Control Server (ACS)	1.4 (Internal EDCS-907015)	November 2012
AGD_OPE	Nexus 7000 Series Switch Operational User Guidance (Common Criteria Specific)	0.7 (Internal EDCS-763642)	November 2012
AGD_PRE	Cisco Nexus 7000 Series Switch Preparative Procedures Wrapper	0.8 (Internal EDCS-763647)	November 2012
AVA_VLA	Section 5.1.5 of this document	-	November 2012
ATE_FUN	Nexus 7000 + ACS Common Criteria Test Documentation (including results)	V1.5 (Internal EDCS-966387)	September 2012

III. Analysis and Testing

Analysis of these changes and regression testing of the product indicated that only minor security functionality was modified so there is minimal security relevance to the modifications. Tables 4 & 5 above summarize the vendor's analysis of the changes.

IV. Conclusion

The changes to the TOE is confined to bug fixes for some minor security functions but mostly non-security functions or features outside the TOA or to elements excluded from the OE. No existing security functionality was removed and no new security functionality was added.