

Mapping of CERT C Secure Coding Standard to Application Security and Development Checklist, version2, release 1.5

Severity Codes

- Category I – assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges
- Category II – assigned to findings that have a potential to lead to unauthorized system access or activity
- Category III – assigned findings that may impact IA posture but are not required to be mitigated or corrected in order for an ATO to be granted

Mapping

CERT C	Check ID	Check Description	Vulnerability Key	Finding Category	Environment	STIG Section	IA Controls
NA	APP2010	System Security plan non-existent or not adequate	V0006197	II	Pre-production & production	2.1.1 System Security Plan 2.1.3 Information Assurance Budget	DCSD-1
NA	APP2020	Application Configuration Guide does not exist	V0016773	II	Pre-production & production	2.1.2 Application Configuration Guide 2.1.4 Security Classification Guide 2.1.5 Mission Assurance Category and Confidentiality 2.2.1 NIAP Approved Products	DCSD-1 DCPB-1 DCSD-1
NA	APP2030	No established IA budget	V0016774	III	Pre-production	2.1.3 Information	DCPB-1

						Assurance Budget	
NA	APP2040	Classification guide does not exist	V0006145	II	Pre-production and production	2.1.4 Security Classification Guide 2.1.5 Mission Assurance Category and Confidentiality	DCSD-1
NA	APP2050	No MAC and CONF levels documented	V0016775	II	Pre-production	2.1.5 Mission Assurance Category and Confidentiality	DCSD-1
CERT C Secure Coding Std	APP2060	No coding standards exist	V0016776	II	Pre-production	2.1.6 Coding Standards 2.2.1 NIAP Approved Products	DCSQ-1
NA	APP2070	Products are not NIAP/Common Criteria approved	V0006170	III	Pre-production	2.2.1 NIAP Approved Products	DCAS-1
NA	APP2080	Products with no or unsuitable robustness profiles	V0016777	II	Pre-production	2.2.2 Robustness Protection Profiles	DCSR-1 DCPD-1 DCPP-1
NA	APP2090	Public domain software in use	V0016778	II	Pre-production	2.2.3 Categories of third party products	DCPD-1
NA	APP2100	Application violates Ports and Protocols Guidance	V0006169	II	Pre-production and production	2.3 Ports and Protocols 2.4.1 Management	DCPP-1
NA	APP2110	Not registered with the DoD Ports and Protocols	V0016779	II	Pre-production and production	2.3 Ports and Protocols 2.4.1 Management 2.5.2 Vulnerability Management Process	DCPP-1
Training	APP2120	Security training not provided	V0016780	II	Pre-production	2.4.1 Management 2.5.2 Vulnerability Management	PRTN-1

						process 2.5.1 Security Incident Response Process 2.6 Workplace Security Procedures	
NA	APP2130	Maintenance does not exist or not sufficient	V0016781	II	Pre-production and production	2.5.2 Vulnerability management Process 2.7 Compliance with DoD Standards	DCCT-1 PESP-1 DCCS-1 DCCS-2 ECSC-1
NA	APP2140	An incident response process is not established	V0016782	II	Pre-production and production	2.5.1 Security Incident Response Process 2.6 Workplace Security Procedures	VIVM-1
NA	APP2150	Inadequate Workplace Security Procedures	V0016783	II	Pre-production and production	2.6 Workplace Security Procedures 2.7 Compliance with DoD Stds	PESP-1
NA	APP2160	Approved Security Configuration Guidance not used	V0006198	II	Pre-production and production	2.7 Compliance with DoD Stds 3.1.1 Design Document	DCCS-1 DCCS-2 ECSC-1
NA	APP3010	Design document is not complete or does not exist	V0007013	II	Pre-production	3.1.1 Design Document	DCFA-1
NA	APP3020	Threat model not established or updated	V0006148	II	Pre-production and production	3.1.3 Threat Model 3.5 Best Practices	DCSQ-1
MSC07-C MSC12-C MSC13-	APP3050	Inactive code and libraries not removed	V0006149	II	Pre-production	3.5 Best Practices	DCSQ-1

C							
NA	APP3060	Application code and data are collocated	V0006150	II	Pre-production	3.5 Best practices	DCPA-1
NA	APP3070	Application components not separated from data storage	V0016784	II	Pre-production and production	3.5 Best Practices	DCPA-1
FIO02-C	APP3080	Invalid URL or path references found	V0006157	II	Pre-production	3.5 Best Practices	DCSQ-1
NA	APP3090	Session hijacking prevention not supported	V0016785	II	Pre-production	3.5 Best Practices	ECTM-2
MEM00-C MEM03-C MEM30-C MEM31-C	APP3100	Temporary objects not removed from system	V0006163	II	Pre-production	3.5 Best Practices	ECRC-1
MSC14-C	APP3110	Unneeded functionality enabled	V0016786	II	Pre-production	3.5.1 Secure Defaults	DCSD-1
ERR00-C ERR01-C ERR02-C ERR03-C ERR04-C ERR05-C ERR06-C ERR30-C ERR31-C ERR32-C	APP3120	Application has error handling vulnerabilities	V006166	II-III	Pre-production	3.5.2 Error Handling	DCSQ-1
ERR00-C ERR04-C ERR05-C PRE09-C	APP3130	Secure design principle not followed	V0016787	I-II	Pre-production	3.5.3 Fail Closed	DCSQ-1
ERR00-C ERR04-C ERR06-C	APP3140	Application failure results in an insecure state	V0006167	II	Pre-production	3.5.3 Fail Closed	DCSS-2
NA	APP3150	Application uses unapproved cryptographic modules	V0006137	II	Pre-production	3.6.1 FIPS 140-2 3.6.4 key Exchange	DCNR-1 ECCR-1 ECCR-2 ECCT-1

							ECCT-2
NA	APP3170	Encryption for Key Exchange not used	V0016788	II	Pre-production	3.6.4 Key Exchange	DCNR-1
NA	APP3180	Encryption key permissions are not adequate	V0016789	II	Pre-production	3.6.4 Key Exchange	ECCD-1
NA	APP3190	Database connections use administrative accounts	V0016790	II	Pre-production	3.7.1 Database Management System	ECLP-1
NA	APP3200	No support for roll-back and journaling	V0016791	III	Pre-production	3.8.1 Database management System	ECDC-1
NA	APP3210	Sensitive data not protected at rest	V006135	II	Pre-production	3.7.2 Data Storage	ECCR-1 ECCR-2
NA	APP3220	Sensitive data is not encrypted in memory	V0016792	II	Pre-production	3.7.3 In-Memory Data Handling	ECCR-1 ECCR-2
MEM00-C MEM03-C MEM09-C MEM31-C	APP3230	Application does not clear all memory blocks	V0016793	II	Pre-production	3.7.3 In-Memory Data Handling	ECCR-1 ECCR-2
FIO06-C FIO11-C FIO15-C FIO16-C FIO30-C	APP3240	Actions not authorized before execution	V0006142	II	Pre-production and production	3.7.3 In-Memory Data Handling	ECRC-1
NA	APP3250	Sensitive data not protected in transit	V0006136	I-II	Pre-production and production	3.7.4 Data Transmission	ECCT-1 ECCT-2 ECNK-1
NA	APP3260	Integrity mechanisms on data files not supported	V0016794	II	Pre-production	3.7.5 Data integrity	ECTM-2 ECML-1
NA	APP3270	Classification labels not appropriately displayed	V0006146	II	Pre-production	3.7.6 Data Marking	ECML-1
NA	APP3280	The application	V0006127	II	Pre-	3.8.3.1 PKI	DCBP-1

		is not PK-enabled			production	User Authentication	IATS-2 IAKM-2 DCNR-1
NA	APP3290	The application utilizes a PKI other than DoD PKI	V0006128	II	Pre-production and production	3.8.3.1 PKI User Authentication 3.8.3.2 PKI Server Authentication	DCBP-1 IATS-2 IAKM-2 DCNR-1
NA	APP3300	Server authentication is not PK-enabled	V0006168	II	Pre-production and production	3.8.3.2 PKI Server Authentication	IATS-1 IATS-2
NA	APP3305	Expired revoked untrusted certificates honored	V0006129	I	Pre-production	3.8.3.3 PKI Certificate Validation	DCBP-1 IATS-2 IAKM-2 DCNR-1
NA	APP3310	Clear text passwords displayed	V0016795	I	Pre-production and production	3.8.4 Password Authentication	IAIA-1
NA	APP3320	Userids have weak passwords	V0006130	II	Pre-production and production	3.8.4.1 Password Complexity and Maintenance 3.8.6 User Accounts	IAIA-1
NA	APP3330	Passwords not transmitted encrypted	V0016796	I	Pre-production	3.8.4.2 Password Transmission	ECCT-1
MSC18-C (wiki version)	APP3340	Passwords stored in an unapproved encrypted format	V0016797	I-II	Pre-production	3.8.4.3 Password Storage	IAIA-1 IAIA-2
MEM06-C	APP3350	Embedded authentication data stored in code	V0006156	I-II	Pre-production and production	3.8.5 Authentication Credentials Protection	IAIA-1 IAIA-2
FIO06-C	APP3360	Authentication data permissions not adequate	V0016798	II-III	Pre-production and production	3.8.5 Authentication Credentials Protection	ECCD-1
NA	APP3370	Unneeded accounts active	V0016799	II	Pre-production	3.8.6 User Accounts	DCSD-1
NA	APP3380	Application	V0006131	II	Pre-	3.8.6 User	IAIA-1

		userid are not unique			production	Accounts	
NA	APP3390	User accounts not locked after invalid logons	V0016800	I	Pre-production and production	3.8.6 User Accounts	ECLO-1
NA	APP3400	User accounts unlocked by person other than admin	V0016801	II	Pre-production	3.8.6 User Accounts	ECLO-1
NA	APP3410	Session limits do not exist for the application	V0006144	II	Pre-production	3.8.7 Sessions	ECLO-1
NA	APP3415	Sessions do not automatically terminate	V0016802	II	Pre-production	3.8.7 Sessions	ECLO-1
NA	APP3420	Explicit logout not available	V0006155	II	Pre-production	3.8.7 Sessions	DCSQ-1
NA	APP3430	Authentication credentials not removed	V0006153	I-II	Pre-production	3.8.7 Sessions	IAIA-1 IAIA-2
NA	APP3440	Logon warning not displayed	V0006152	II	Pre-production	3.8.8 Logon Banner	ECWM-1
FIO06-C FIO15-C	APP3450	Application resources has inappropriate permission	V0016803	II	Pre-production and production	3.9 Access Control 3.9.1 Name Resolution	ECCD-1
FIO11-C	APP3460	Resource name used to control access	V0016804	I	Pre-production	3.9.1 Name Resolution	DCSQ-1
NA	APP3470	Application functionality not role based	V0006154	II	Pre-production and production	3.9.2 Role Based Access	ECPA-1 ECCD-2
FIO06-C	APP3480	Access control mechanism not in place	V0006141	II	Pre-production and production	3.9.2 Role Based Access 3.1 Input Validation	ECCD-2 ECLP-1 DCSQ-1
NA	APP3500	Application runs with excessive privileges	V0006143	II	Pre-production	3.9.3 Excessive Privileges	ECLP-1
INT04-C INT05-C STR02-C STR08-C STR35-C STR36-C	APP3510	Insufficient input validation	V0006164	I-II	Pre-production	3.1 Input Validation	DCSQ-1

MEM35-C							
NA	APP3520	No Trust boundary data validation	V0016805	II	Pre-production	3.1 Input Validation	DCSQ-1
NA	APP3530	Application does not set character set	V0016806	II	Pre-production	3.1 Input Validation	DCSQ-1
NA	APP3540	Application is vulnerable to SQL Injection	V0016807	I-II	Pre-production	3.10.1 SQL Injection Vulnerabilities	DCSQ-1
INT02-C INT04-C INT05-C INT08-C INT32-C	APP3550	Application is vulnerable to integer overflows	V0016808	I	Pre-production	3.10.2 Integer Arithmetic Vulnerabilities	DCSQ-1
STR01-C STR02-C STR31-C STR35-C STR36-C	APP3560	Application contains format string vulnerabilities	V0016809	I	Pre-production	3.10.3 Format String Vulnerabilities	DCSQ-1
ENV04-C	APP3570	Application vulnerable to Command Injection	V0016810	I	Pre-production	3.10.4 Command Injection Vulnerabilities	DCSQ-1
NA	APP3580	Application vulnerable to Cross Site Scripting	V0016811	I	Pre-production	3.10.5 Cross Site Scripting (XSS) Vulnerabilities	DCSQ-1
ARR02-C ARR30-C ARR33-C STR01-C STR31-C STR35-C STR36-C	APP3590	Application is vulnerable to buffer overflows	V0006165	I	Pre-production	3.10.6 Buffer Overflow Vulnerabilities	DCSQ-1
FIO02-C	APP3600	Vulnerable to canonical representation attacks	V0016812	II	Pre-production	3.11 Canonical Representation	DCSQ-1
NA	APP3610	Hidden fields used to control access privileges	V0016813	I-II	Pre-production	3.12 Hidden Fields in Web Pages	DCSQ-1
NA	APP3620	Application discloses unnecessary information	V0016814	II	Pre-production	3.13 Application Information Disclosure	ECCD-1

POS00-C POS31-C POS35-C	APP3630	Application vulnerable to race conditions	V0016815	II	Pre-production	3.14 Race Conditions	DCSQ-1
NA	APP3640	No logs for data access and changes	V0016816	II	Pre-production	3.15 Auditing	ECCD-2
ERR00-C MSC31-C	APP3650	No warning when logs are near full	V0006139	III	Pre-production	3.15.1 Audit Notifications	ECAT-2
NA	APP3660	Last login information not displayed	V0016817	III	Pre-production	3.15.1 Audit Notifications	ECLO-2
NA	APP3670	No notification of time of last change of data	V0016818	II	Pre-production	3.15.1 Audit Notifications	ECCD-2
NA	APP3680	The application does not adequately log events	V0006138	II	Pre-production	3.15.2 Access for Need-to-Know 3.16.1.1 Category 1A Mobile Code 3.16.2.1 Category 2 Mobile Code in Constrained Environment 3.16.4 Emerging Mobile Code	ECAR-1 ECAR-2 ECAR-3
NA	APP3690	Application audit logs have incorrect permissions	V0006140	II	Pre-production and production	3.15.5 Audit Trail Protection 3.16.2.1 Category 2 Mobile Code in Constrained Environment	ECTP-1
NA	APP3700	Unsigned Cat 1A or 2 mobile code in use	V0006159	II	Pre-production	3.16.1.1 Category 1A Mobile Code 3.16.4 Emerging mobile Code 3.16.5 New Procurement and Development	DCMC-1

						Efforts	
NA	APP3710	Mobile code executed without verifying signature	V0006161	II	Pre-production	3.16.1.1 Category 1A Mobile Code 3.16.2.1 Category 2 Mobile Code in Constrained Environment	DCMC-1
NA	APP3720	Unsigned unconstrained mobile code used	V0006160	II	Pre-production	3.16.2.1 Category 2 Mobile Code in Constrained Environment	DCMC-1
NA	APP3730	Uncategorized mobile code used	V0006162	II	Pre-production	3.16.4 Emerging Mobile Code	DCMC-1
NA	APP3740	Code sent in email	V0006158	II	Pre-production	3.16.4 Emerging Mobile Code	DCMC-1
NA	APP3750	New mobile development not compliant DoDI 5200.40	V0016819	II	Pre-production	3.16.5 New Procurement and Development Efforts	DCMC-1
NA	APP4010	Access rights to the CM repository not reviewed	V0016820	III	Pre-production	4 Software Configuration Management	ECPC-1 ECPC-2
NA	APP4020	Flaws found during a code review are not tracked	V0016821	III	Pre-production	4 Software Configuration Management	DCSQ-1
NA	APP4030	The SCM plan does not exist	V0016822	II-III	Pre-production	4.1 Software Configuration Management Plan	DCCS-2
NA	APP4040 A	Configuration Control Board does not exist	V0016823	II-III	Pre-production	4.2 Configuration Control Board	DCCB-1 ECRC-1
Training	APP5010	No tester designated to test for security flaws	V0016824	III	Pre-production	5 Testing	DCSQ-1
NA	APP5030	Data files modified outside the	V0006147	II	Pre-production	5 Testing	ECRC-1

		application					
Training	APP5040	Changes to the application are not assessed for IA	V0016825	II	Pre-production	5 Testing	DCII-1
NA	APP5050	Tests plans not executed prior to release or patch	V0016826	II	Pre-production	5.1 Test Plans and Procedures	DCCS-2
NA	APP5060	System in insecure state during startup and shutdown	V0016827	II	Pre-production	5.1 Test Plans and Procedures	DCCS-2
NA	APP5070	Application has no code coverage statistics	V0016828	III	Pre-production	5.3 Code coverage	DCSQ-1
Training	APP5080	Code reviews not performed prior to release	V0016829	II	Pre-production	5.4 Code Reviews	DCSQ-1
NA	APP5090	Flaws found during a code review are not tracked	V0016830	II	Pre-production	5.4 Code Reviews	DCSQ-1
NA	APP5100	Fuzz testing is not performed	V0016831	III	Pre-production	5.2 Fuzz Testing	DCSQ-1
NA	APP5110	Security flaws not addressed in project plan	V0016832	II	Pre-production	5.2 Fuzz Testing	DCSQ-1
NA	APP6010	Critical application hosted on a multi-use server	V0016833	II	Production	6.1.3 Application Configuration Guide	DCSQ-1
NA	APP6020	COTS products not configured to best practices	V0016834	II	Production	6.2 Third Party Software	DCCS-1
NA	APP6030	Unnecessary services or software not removed	V0006151	II	Production	6.5 Unnecessary Services	DCSD-1
NA	APP6040	Administrator has not registered to updates	V0016835	II	Production	6.6.1 Vulnerability Management	DCCT-1
NA	APP6050	Current patches and configurations	V0016836	II	Production	6.6.1 Vulnerability Management	DCCT-1

		not installed					
NA	APP6060	App not decommissioned when maintenance is expired	V0016837	III	Production	6.6.2 Maintenance Availability	DCSD-1
NA	APP6070	No procedures exist to decommission application	V0016838	III	Production	6.6.2 Maintenance Availability	DCSD-1
NA	APP6080	Protections against DoS attacks not implemented	V0016839	II	Production	6.8 Denial of Service	DCSQ-1
NA	APP6090	No system alerts in a low resource condition	V0016840	III	Production	6.8 Denial of Service	ECAT-2
NA	APP6100	Sensitive data not purged from production export	V0006174	II	Production	6.1 Database Exports	ECAN-1
NA	APP6110	Audit trail not periodically reviewed	V0016841	III	Production	6.12.1 Audit Trail Monitoring	ECCD-2
NA	APP6120	IAO has no process to report IA violations	V0016842	II	Production	6.12.1 Audit Trail Monitoring	ECAT-2
NA	APP6130	No automated audit trail monitoring	V0016843	III	Production	6.12.1 Audit Trail Monitoring	ECAT-2
NA	APP6140	Log files are not retained for at least one year	V0006173	II	Production	6.12.2 Audit Log Retention	ECRR-1
NA	APP6160	Disaster recovery plan does not exist	V0006171	II	Production	6.13 Recovery and Contingency Planning	COTR-1
NA	APP6170	Application backups not in fire rated container	V0016844	II	Production	6.13 Recovery and Contingency Planning	COSW-1
NA	APP6180	Backup and restoration device not protected	V0016845	II	Production	6.13 Recovery and Contingency Planning	COBR-1

NA	APP6190	Backups or backup procedures are incomplete	V0006172	II	Production	6.13 Recovery and Contingency Planning	CODB-3 CODP-3 IAAC-1
NA	APP6200	Disaster plan does not exist or is incomplete	V0016846	II	Production	6.13 Recovery and Contingency Planning	CODP-3
NA	APP6210	No account management process in place	V0016847	II	Production	6.14 Account Management	IAAC-1
NA	APP6220	Generated passwords do not comply with policy	V0016848	II	Production	6.14 Account Management	IAIA-1 IAIA-2
NA	APP6230	Access granted by group authenticator	V0016849	II	Production	6.14 Account Management	IAGA-1
NA	APP6240	Inactive userids are not disabled	V0006132	III	Production	6.14 Account Management	IAIA-1
NA	APP6250	Unnecessary built-in userids are not disabled	V0006133	II	Production	6.14 Account Management	IAIA-1
NA	APP6260	Userids have default passwords	V0006134	I-II	Production	6.14 Account Management	IAIA-1
NA	APP6270	DMZ not present between DoD and public networks	V0016850	II	Production	6.15 Deployment Infrastructure	EBPW-1

Version 0 – 10/14/09

Version 0.1 – 10/15/09 – Robert Seacord provided inputs on APP3060, APP3140, APP3340. Highlighted STIG checks that Jeremy had identified as being applicable to the CERT C Secure Coding Standard.

Version 1.0 – 12/04/09 – No additional comments had been received from Jeremy, so I removed the highlights.