Checkmarx CxSAST

New and Updated Vulnerability Queries for 8.9.0

October, 2018

Contents

VULNERABILITY QUERIES **4**

Vulnerability Queries

The following vulnerability queries are either new or were updated for v8.9.0

Language	Package	Query	CWE ID	Status
ASP	ASP_High_Risk	SQL_Injection	89	Update
ASP	ASP_Medium_Threat	SQL_Injection_Evasion_Attack	89	Update
ASP	ASP_Medium_Threat	Unclosed_Connection	404	Update
ASP	ASP_Heuristic	Heuristic_2nd_Order_SQL_Injection	89	Update
ASP	ASP_Heuristic	Heuristic_SQL_Injection	89	Update
ASP	ASP_Low_Visibility	Blind_SQL_Injections	89	Update
ASP	ASP_Low_Visibility	Session_Poisoning	472	Update
ASP	ASP_Best_Coding_Practice	Dynamic_SQL_Queries	89	Update
CPP	CPP_Buffer_Overflow	Buffer_Overflow_LongString	120	Update
CPP	CPP_Medium_Threat	Divide_By_Zero	369	Update
CPP	CPP_Medium_Threat	Double_Free	415	Update
CPP	CPP_Medium_Threat	MemoryFree_on_StackVariable	590	Update
CPP	CPP_Medium_Threat	Use_After_Free	416	Update
CPP	CPP_Weak_Cryptography	Asymmetric_Encryption_RSA_Low_Public_Exponent	326	New
CPP	CPP_Weak_Cryptography	Encoding_Used_Instead_of_Encryption	311	Update
CPP	CPP_Heuristic	Heuristic_Buffer_Improper_Index_Access	129	New
CPP	CPP_Low_Visibility	Arithmetic_Operation_On_Boolean	398	Update
CPP	CPP_Low_Visibility	Creation_of_chroot_Jail_without_Changing_Working_Directory	243	Update
CPP	CPP_Best_Coding_Practice	Buffer_Size_Literal_Condition	118	Update
CPP	CPP_MISRA_C	R12_05_AND_OR_Operands_Not_As_Primary_Expressions	0	Update
CPP	CPP_MISRA_C	R14_04_Use_Of_Goto	0	Update
CPP	CPP_MISRA_C	R14_05_Use_Of_Continue	0	Update
CPP	CPP_MISRA_C	R15_02_Non_Empty_Switch_Clause_Without_Break	0	Update
CPP	CPP_MISRA_C	R16_01_Function_With_Variable_Number_Of_Arguments	0	Update

Language	Package	Query	CWE ID	Status
CPP	CPP_MISRA_C	R18_04_Use_Of_Union	0	Update
CPP	CPP_MISRA_C	R19_01_Non_Prepocessor_Command_Before_Include_In_File	0	Update
CPP	CPP_MISRA_C	R20_05_Using_Errno_Indicator_From_Errno_H	0	Update
CPP	CPP_MISRA_C	R20_06_Using_Offsetof_Macro_From_Stddef_H	0	Update
CPP	CPP_MISRA_C	R20_07_Using_Setjmp_Longjmp_Macros_From_Setjmp_H	0	Update
CPP	CPP_MISRA_C	R20_08_Using_Signal_Handling_From_Signal_H	0	Update
CPP	CPP_MISRA_C	R20_09_Using_Input_Output_From_Stdio_H	0	Update
CPP	CPP_MISRA_C	R20_10_Using_Atof_Atoi_Atol_Functions_From_Stdlib_H	0	Update
CPP	CPP_MISRA_C	R20_11_Using_Abort_Exit_Getenv_System_Functions_From_Stdlib_H	0	Update
CPP	CPP_MISRA_C	R20_12_Using_Time_Handling_From_Time_H	0	Update
CPP	CPP_MISRA_CPP	R09_05_01_Use_Of_Union	0	Update
CPP	CPP_MISRA_CPP	R15_01_02_No_Explicit_Null_Throw	10764	Update
CPP	CPP_MISRA_CPP	R15_03_03_Accessing_Non_Static_Mem_In_Ctr_Dtr	10767	Update
CPP	CPP_MISRA_CPP	R18_00_04_Ctime	0	Update
CPP	CPP_MISRA_CPP	R18_00_05_Unbounded_Functions_Of_Library_CString	0	Update
CPP	CPP_MISRA_CPP	R18_07_01_Csignal	0	Update
CSharp	CSharp_High_Risk	SQL_Injection	89	Update
CSharp	CSharp_Medium_Threat	Cookie_Injection	20	Update
CSharp	CSharp_Medium_Threat	Integer_Overflow	190	Update
CSharp	CSharp_Medium_Threat	Privacy_Violation	359	Update
CSharp	CSharp_Medium_Threat	SQL_Injection_Evasion_Attack	89	Update
CSharp	CSharp_Medium_Threat	Unclosed_Connection	404	Update
CSharp	CSharp_Low_Visibility	Blind_SQL_Injections	89	Update
CSharp	CSharp_Low_Visibility	Improper_Resource_Shutdown_or_Release	404	Update
CSharp	CSharp_Low_Visibility	Missing_Content_Security_Policy	346	New
CSharp	CSharp_Low_Visibility	Session_Poisoning	472	Update
CSharp	CSharp_Low_Visibility	Stored_Code_Injection	94	New
CSharp	CSharp_Best_Coding_Practice	Declaration_Of_Catch_For_Generic_Exception	396	Update
CSharp	CSharp_Best_Coding_Practice	Unchecked_Return_Value	252	Update

Language	Package	Query	CWE ID	Status
Go	Go_High_Risk	CGI_XSS	79	Update
Go	Go_High_Risk	Deserialization_of_Untrusted_Data	502	Update
Go	Go_Medium_Threat	Hardcoded_Password_in_Connection_String	547	New
Go	Go_Medium_Threat	SSRF	918	Update
Go	Go_Low_Visibility	Race_Condition_In_Cross_Functionality	362	New
Go	Go_Low_Visibility	Use_of_Hardcoded_Password	259	New
Groovy	Groovy_High_Risk	Second_Order_SQL_Injection	89	Update
Groovy	Groovy_High_Risk	SQL_Injection	89	Update
Groovy	Groovy_Medium_Threat	SQL_Injection_Evasion_Attack	89	Update
Groovy	Groovy_Medium_Threat	Use_of_Hard_coded_Cryptographic_Key	321	Update
Groovy	Groovy_Heuristic	Heuristic_2nd_Order_SQL_Injection	89	Update
Groovy	Groovy_Heuristic	Heuristic_SQL_Injection	89	Update
Groovy	Groovy_Low_Visibility	Blind_SQL_Injections	89	Update
Groovy	Groovy_Low_Visibility	Improper_Exception_Handling	248	Update
Groovy	Groovy_Low_Visibility	Parse_Double_DoS	730	Update
Groovy	Groovy_Low_Visibility	Unchecked_Return_Value_to_NULL_Pointer_Dereference	690	Update
Groovy	Groovy_Low_Visibility	Unsynchronized_Access_To_Shared_Data	567	Update
Groovy	Groovy_Best_Coding_Practice	Dynamic_SQL_Queries	89	Update
Groovy	Groovy_Best_Coding_Practice	Omitted_Break_Statement_In_Switch	484	Update
Groovy	Groovy_Best_Coding_Practice	Use_Collect_Nested	398	Update
Java	Java_Android	Insufficient_Sensitive_Transport_Layer	319	Update
Java	Java_Android	Malicious_Program	265	Update
Java	Java_High_Risk	Expression_Language_Injection_SPEL	917	New
Java	Java_High_Risk	Second_Order_SQL_Injection	89	Update
Java	Java_High_Risk	SQL_Injection	89	Update
Java	Java_Android	Exported_Service_Without_Permissions	668	Update
Java	Java_Android	Failure_To_Implement_Least_Privilege	250	Update
Java	Java_Medium_Threat	CGI_Reflected_XSS_All_Clients	79	Update
Java	Java_Medium_Threat	CGI_Stored_XSS	79	Update

Language	Package	Query	CWE ID	Status
Java	Java_Medium_Threat	SQL_Injection_Evasion_Attack	89	Update
Java	Java_Medium_Threat	Unchecked_Input_for_Loop_Condition	606	Update
Java	Java_Medium_Threat	Use_of_Hard_coded_Cryptographic_Key	321	Update
Java	Java_Medium_Threat	XSRF	352	Update
Java	Java_Struts	Struts_Form_Does_Not_Extend_Validation_Class	104	Update
Java	Java_Struts	Struts_Incomplete_Validate_Method_Definition	103	Update
Java	Java_Struts	Struts_Validation_Turned_Off	109	Update
Java	Java_Android	Accessible_Content_Provider	668	Update
Java	Java_Android	Debuggable_App	668	Update
Java	Java_Android	Hardcoded_Password_In_Gradle	259	Update
Java	Java_Android	Insecure_Android_SDK_Version	477	Update
Java	Java_Android	Missing_Certificate_Pinning	295	Update
Java	Java_Android	Missing_Device_Lock_Verification	829	Update
Java	Java_Android	ProGuard_Obfuscation_Not_In_Use	693	Update
Java	Java_Low_Visibility	Blind_SQL_Injections	89	Update
Java	Java_Low_Visibility	Citrus_Developer_Mode_Enabled	0	New
Java	Java_Low_Visibility	Hardcoded_AWS_Credentials	798	New
Java	Java_Low_Visibility	Improper_Resource_Access_Authorization	285	Update
Java	Java_Low_Visibility	Log_Forging	117	Update
Java	Java_Low_Visibility	Unchecked_Return_Value_to_NULL_Pointer_Dereference	690	Update
Java	Java_Low_Visibility	Uncontrolled_Memory_Allocation	789	Update
Java	Java_Low_Visibility	Unsynchronized_Access_To_Shared_Data	567	Update
Java	Java_Potential	Potential_SQL_Injection	89	Update
Java	Java_Struts	Struts_Duplicate_Config_Files	694	Update
Java	Java_Struts	Struts_Duplicate_Form_Bean	694	Update
Java	Java_Struts	Struts_Duplicate_Validation_Files	694	Update
Java	Java_Struts	Struts_Duplicate_Validation_Forms	102	Update
Java	Java_Struts	Struts_Form_Field_Without_Validator	105	Update
Java	Java_Struts	Struts_Mapping_to_Missing_Form_Bean	457	Update

Language	Package	Query	CWE ID	Status
Java	Java_Struts	Struts_Non_Private_Field_In_ActionForm_Class	608	Update
Java	Java_Struts	Struts_Thread_Safety_Violation_In_Action_Class	856	Update
Java	Java_Struts	Struts_Unused_Validation_Form	107	Update
Java	Java_Struts	Struts_Unvalidated_Action_Form	108	Update
Java	Java_Struts	Struts_Validator_Without_Form_Field	110	Update
Java	Java_Struts	Struts2_Action_Field_Without_Validator	108	Update
Java	Java_Struts	Struts2_Duplicate_Action_Field_Validators	102	Update
Java	Java_Struts	Struts2_Duplicate_Validators	102	Update
Java	Java_Android	Allowed_Backup	0	Update
Java	Java_Best_Coding_Practice	Dynamic_SQL_Queries	89	Update
Java	Java_Best_Coding_Practice	Null_Pointer_Dereference	476	Update
Java	Java_Best_Coding_Practice	Omitted_Break_Statement_In_Switch	484	Update
Java	Java_Best_Coding_Practice	Portability_Flaw_In_File_Separator	474	Update
Java	Java_Best_Coding_Practice	Reachable_Assertion	617	Update
Java	Java_Best_Coding_Practice	Unchecked_Return_Value	252	Update
Java	Java_Best_Coding_Practice	Use_of_Obsolete_Functions	477	Update
Java	Java_Best_Coding_Practice	Use_Of_Uninitialized_Variables	457	Update
Java	Java_Struts	Struts_Missing_Form_Bean_Name	563	Update
Java	Java_Struts	Struts_Missing_Form_Bean_Type	563	Update
Java	Java_Struts	Struts_Missing_Forward_Name	489	Update
Java	Java_Struts	Struts_Unused_Action_Form	489	Update
Java	Java_Struts	Struts_Use_of_Relative_Path_in_Config	21	Update
Java	Java_Struts	Struts2_Undeclared_Validator	105	Update
Java	Java_Struts	Struts2_Validation_File_Without_Action	107	Update
Java	Java_Struts	Struts2_Validator_Without_Action_Field	110	Update
JavaScript	Javascript_XS	XS_Code_Injection	94	Update
JavaScript	Javascript_XS	XS_Reflected_XSS	79	Update
JavaScript	Javascript_XS	XS_Second_Order_SQL_Injection	89	Update
JavaScript	Javascript_XS	XS_SQL_Injection	89	Update

Language	Package	Query	CWE ID	Status
JavaScript	Javascript_XS	XS_Stored_Code_Injection	94	Update
JavaScript	Javascript_XS	XS_Stored_XSS	79	Update
JavaScript	Javascript_XS	XS_Open_Redirect	601	Update
JavaScript	Javascript_XS	XS_Parameter_Tampering	472	Update
JavaScript	Javascript_XS	XS_Response_Splitting	113	Update
JavaScript	Javascript_XS	XS_Use_Of_Hardcoded_URL	798	Update
JavaScript	Javascript_XS	XS_XSRF	352	Update
JavaScript	JavaScript_Server_Side_Vulnerabilities	Divide_By_Zero	369	Update
JavaScript	Javascript_XS	XS_Log_Injection	117	Update
JavaScript	Javascript_XS	XS_Overly_Permissive_CORS	749	Update
JavaScript	Javascript_XS	XS_Potentially_Vulnerable_To_Clickjacking	693	Update
JavaScript	Javascript_XS	XS_Unencrypted_Data_Transfer	319	Update
JavaScript	JavaScript_Server_Side_Vulnerabilities	Omitted_Break_Statement_In_Switch	484	Update
Objc	ObjectiveC_High_Risk	Second_Order_SQL_Injection	89	Update
Objc	ObjectiveC_High_Risk	SQL_Injection	89	Update
Objc	ObjectiveC_Low_Visibility	Missing_Device_Lock_Verification	829	Update
Objc	ObjectiveC_Best_Coding_Practice	Dynamic_SQL_Queries	89	Update
Perl	Perl_High_Risk	SQL_Injection	89	Update
Perl	Perl_Low_Visibility	Variables_Outside_The_Scope_of_a_Regex	824	Update
PHP	PHP_High_Risk	File_Disclosure	538	Update
PHP	PHP_High_Risk	File_Inclusion	98	Update
PHP	PHP_High_Risk	File_Manipulation	552	Update
PHP	PHP_Medium_Threat	Stored_File_Inclusion	98	Update
PHP	PHP_Medium_Threat	Stored_File_Manipulation	552	Update
PLSQL	PLSQL_High_Risk	SQL_Injection	89	Update
Python	Python_High_Risk	Command_Injection	77	Update
Python	Python_High_Risk	LDAP_Injection	90	Update
Python	Python_High_Risk	Second_Order_SQL_Injection	89	Update
Python	Python_High_Risk	SQL_Injection	89	Update

Language	Package	Query	CWE ID	Status
Python	Python_Medium_Threat	Stored_LDAP_Injection	90	Update
Python	Python_Low_Visibility	Missing_Content_Security_Policy	346	New
Python	Python_Low_Visibility	Stored_Code_Injection	94	New
Ruby	Ruby_High_Risk	Second_Order_SQL_Injection	89	Update
Ruby	Ruby_High_Risk	SQL_Injection	89	Update
Ruby	Ruby_Medium_Threat	Privilege_Escalation	285	Update
Ruby	Ruby_Low_Visibility	Blind_SQL_Injections	89	Update
Ruby	Ruby_Best_Coding_Practice	Dynamic_SQL_Queries	89	Update
Scala	Scala_High_Risk	Second_Order_SQL_Injection	89	Update
Scala	Scala_High_Risk	SQL_Injection	89	Update
Scala	Scala_Medium_Threat	SQL_Injection_Evasion_Attack	89	Update
VB6	VB6_High_Risk	Second_Order_SQL_Injection	89	Update
VB6	VB6_High_Risk	SQL_Injection	89	Update
VB6	VB6_Heuristic	Heuristic_SQL_Injection	89	Update
VB6	VB6_Low_Visibility	Stored_Code_Injection	94	New
VbNet	VbNet_High_Risk	Code_Injection	94	Update
VbNet	VbNet_High_Risk	Resource_Injection	99	Update
VbNet	VbNet_High_Risk	Second_Order_SQL_Injection	89	Update
VbNet	VbNet_High_Risk	SQL_Injection	89	Update
VbNet	VbNet_High_Risk	UTF7_XSS	79	Update
VbNet	VbNet_Medium_Threat	Buffer_Overflow	120	Update
VbNet	VbNet_Medium_Threat	Cross_Site_History_Manipulation	203	Update
VbNet	VbNet_Medium_Threat	DB_Parameter_Tampering	284	Update
VbNet	VbNet_Medium_Threat	DoS_by_Sleep	730	Update
VbNet	VbNet_Medium_Threat	Hardcoded_password_in_Connection_String	547	Update
VbNet	VbNet_Medium_Threat	Heap_Inspection	244	Update
VbNet	VbNet_Medium_Threat	HTTP_Response_Splitting	113	Update
VbNet	VbNet_Medium_Threat	Improper_Locking	667	Update
VbNet	VbNet_Medium_Threat	Integer_Overflow	190	Update

Language	Package	Query	CWE ID	Status
VbNet	VbNet_Medium_Threat	No_Request_Validation	20	Update
VbNet	VbNet_Medium_Threat	Path_Traversal	36	Update
VbNet	VbNet_Medium_Threat	Privacy_Violation	359	Update
VbNet	VbNet_Medium_Threat	Reflected_XSS_Specific_Clients	79	Update
VbNet	VbNet_Medium_Threat	SQL_Injection_Evasion_Attack	89	Update
VbNet	VbNet_Medium_Threat	Trust_Boundary_Violation	501	Update
VbNet	VbNet_Medium_Threat	Unclosed_Connection	404	Update
VbNet	VbNet_Medium_Threat	Unsafe_Object_Binding	915	Update
VbNet	VbNet_Medium_Threat	Use_of_Hard_coded_Cryptographic_Key	321	Update
VbNet	VbNet_Medium_Threat	XSRF	352	Update
VbNet	VbNet_Heuristic	Heuristic_2nd_Order_SQL_Injection	89	Update
VbNet	VbNet_Heuristic	Heuristic_SQL_Injection	89	Update
VbNet	VbNet_Low_Visibility	Blind_SQL_Injections	89	Update
VbNet	VbNet_Low_Visibility	Cleansing_Canonicalization_and_Comparison_Errors	171	Update
VbNet	VbNet_Low_Visibility	Client_Side_Only_Validation	602	Update
VbNet	VbNet_Low_Visibility	Dangerous_File_Upload	434	Update
VbNet	VbNet_Low_Visibility	Hardcoded_Absolute_Path	426	Update
VbNet	VbNet_Low_Visibility	Impersonation_Issue	520	Update
VbNet	VbNet_Low_Visibility	Improper_Resource_Shutdown_or_Release	404	Update
VbNet	VbNet_Low_Visibility	Improper_Session_Management	201	Update
VbNet	VbNet_Low_Visibility	Improper_Transaction_Handling	460	Update
VbNet	VbNet_Low_Visibility	Information_Exposure_Through_an_Error_Message	209	Update
VbNet	VbNet_Low_Visibility	Information_Leak_Through_Persistent_Cookies	539	Update
VbNet	VbNet_Low_Visibility	Insufficiently_Protected_Credentials	522	Update
VbNet	VbNet_Low_Visibility	Just_One_of_Equals_and_Hash_code_Defined	581	Update
VbNet	VbNet_Low_Visibility	Leaving_Temporary_Files	376	Update
VbNet	VbNet_Low_Visibility	Open_Redirect	601	Update
VbNet	VbNet_Low_Visibility	Session_Clearing_Problems	613	Update
VbNet	VbNet_Low_Visibility	Session_Poisoning	472	Update

Language	Package	Query	CWE ID	Status
VbNet	VbNet_Low_Visibility	Stored_Code_Injection	94	New
VbNet	VbNet_Low_Visibility	Thread_Safety_Issue	567	Update
VbNet	VbNet_Low_Visibility	URL_Canonicalization_Issue	647	Update
VbNet	VbNet_Low_Visibility	Use_of_Broken_or_Risky_Cryptographic_Algorithm	327	Update
VbNet	VbNet_Low_Visibility	Use_Of_Hardcoded_Password	259	Update
VbNet	VbNet_Low_Visibility	XSS_Evasion_Attack	79	Update
VbNet	VbNet_WebConfig	Password_In_Configuration_File	260	Update
VbNet	VbNet_Best_Coding_Practice	Catch_NullPointerException	395	Update
VbNet	VbNet_Best_Coding_Practice	Declaration_Of_Catch_For_Generic_Exception	396	Update
VbNet	VbNet_Best_Coding_Practice	Direct_Use_of_Sockets	246	Update
VbNet	VbNet_Best_Coding_Practice	Dynamic_SQL_Queries	89	Update
VbNet	VbNet_Best_Coding_Practice	Exposure_of_Resource_to_Wrong_Sphere	493	Update
VbNet	VbNet_Best_Coding_Practice	GetLastWin32Error_Is_Not_Called_After_Pinvoke	10018	Update
VbNet	VbNet_Best_Coding_Practice	Hardcoded_Connection_String	798	Update
VbNet	VbNet_Best_Coding_Practice	Leftover_Debug_Code	489	Update
VbNet	VbNet_Best_Coding_Practice	Magic_Numbers	0	Update
VbNet	VbNet_Best_Coding_Practice	Missing_XML_Validation	112	Update
VbNet	VbNet_Best_Coding_Practice	NULL_Argument_to_Equals	0	Update
VbNet	VbNet_Best_Coding_Practice	Pages_Without_Global_Error_Handler	544	Update
VbNet	VbNet_Best_Coding_Practice	PersistSecurityInfo_is_True	0	Update
VbNet	VbNet_Best_Coding_Practice	Threads_in_WebApp	383	Update
VbNet	VbNet_Best_Coding_Practice	Unchecked_Error_Condition	391	Update
VbNet	VbNet_Best_Coding_Practice	Unchecked_Return_Value	252	Update
VbNet	VbNet_Best_Coding_Practice	Unclosed_Objects	459	Update
VbNet	VbNet_Best_Coding_Practice	Unvalidated_Arguments_Of_Public_Methods	0	Update
VbNet	VbNet_Best_Coding_Practice	Use_of_System_Output_Stream	398	Update
VbNet	VbNet_Best_Coding_Practice	Use_Of_Uninitialized_Variables	457	Update
VbNet	VbNet_Best_Coding_Practice	Visible_Pointers	0	Update