datacap systems, inc.

Engineering Department
Code Review Checklist

Developer: Bob Carleone

Review Completed: 7/29/2015

Project/Product: NETePay 5 Paymentech Term DEV

Version: 5.06.10

Source Location: DSINetConnectIP_Term50610_DEV

Reviewer: Lee Morsillo

Reviewer: Joe Van Lente

Project Security Advisor: Dennis Fillenwarth

Note: Review process requires that Reviewers listed above are other than the originating code author and are knowledgeable about product(s) to be reviewed and secure coding practices.

Legends: NA = Not Applicable
OK = No issues identified
NR = Needs further review. See reviewer's notes.

NA	OK	NR	***Buffer Overrun***
	X		Check for usage of unsafe string handling functions.
	X		Undefine strcpy, strcat, sprintf, and similar functions and let compiler identify.
	X		Identify allocations and examine arithmetic used to calculate buffer size.
	X		Trace user input from entry points through all function calls.

NA	OK	NR	***SQL Injection***
	X		Identify where queries are performed and determine that data trustworthiness used in each query.
X			Identify areas where SQL statements are executed and determine if string concatenation or replacement is used on untrusted data.

NA	OK	NR	***Format String Vulnerabilities***
	X		Identify and review function definitions that include … in the argument list for problems.

NA	OK	NR	***Integer Overflow***
	X		Check all input before manipulation.
	X		Identify areas which manipulate memory directly and examine size checking math.
	X		Investigate called functions down to low-level runtime or system calls if possible.
	X		Investigate sources of arguments and determine if tampering can be detected or that arguments are under exclusive application control.

NA	OK	NR	***Command Injection***
	X		Identify constructs that could be used to invoke any kind of command processor. Check for suitable defensive measures in any identified calls – avoid deny-list-based approaches in favor of allow-list-based approaches.

NA	OK	NR	***Error Handling***
	X		Identify Exception, Try and Catch and Finally key words and verify exceptions are being handled appropriately.

NA	OK	NR	***Protect Network Traffic***
	X		Verify that confidentiality for a particular connection is effective.

	X		Use well known algorithms for underlying cryptographic ciphers.
	X		Verify that underlying key material is not obvious.
	X		Do not reuse keys with stream cyphers.
	X		Make sure that message authentication applies to every message. And that it is used on the receives side.
X			Verify that authentication schemes are used to prevent capture-replay attacks.
	X		Verify that encryption keys are not doing double duty as message authentication keys.

NA	OK	NR	***Proper Use of SSL and TLS***
	X		Identify input points from the network and verify whether code is using SSL/TLS.

NA	OK	NR	***Store and Protect Data Securely***
	X		Identify and evaluate any code that sets access controls or permissions. Identify code that creates other objects or creates files and does not set access control. Evaluate whether default access controls are sufficient for sensitivity of information.
X			Determine if keywords such as Secret, Private, Password, Pwd, Key, Passphrase, Crypt or Cypher are related to embedded secret data and if so, assure that the secret is not within the code itself.

NA	OK	NR	***Information Leakage***
	X		Use least precision possible in time stamps included with data for crypto operations.

NA	OK	NR	***Improper File Access***
			Identify all file I/O functions that use filenames and review the following:
X			Determine where filename originates and whether it is trusted.
	X		Is the filename being used more than once to access and manipulate data?
X			Is the file in a place on the file system that attackers can potentially access?
X			Is there a way for an attacker to manipulate the filename to point to a file that shouldn't be accessed?

NA	OK	NR	***Trusting Network Name Resolution***
	X		Avoid using UDP, use TCP.

NA	OK	NR	***Race Conditions***
	X		Evaluate signal handlers, including the data they manipulate.
	X		Use Windows API calls like CreateFile when possible

NA	OK	NR	***Unauthenticated Key Exchange***
	X		Implement basic network protection at network communications points. Implement protocol for authentication on session connections.
	X		Verify that authentication protocols result in a key by looking at the protocol outputs. If it doesn't, check to ensure that the protocol is authenticating data from the key exchange. If there is an exchanged key, verify whether it is used as the foundation for ongoing link protection.
	X		Ensure that authentication messages can't be spoofed. If authentication can be attacked, verify that its only the first successful login, or whether it's true for future logins.

NA	OK	NR	***Cryptographically Strong Random Numbers***
	X		Determine where random numbers should be used.
	X		Identify code that uses PRNGs.

	X		For code that uses CPRGs, verify that they're seeded properly.

NA	OK	NR	***Usability***
	X		Identify security options in UI code. Verify that any default settings are appropriate and convey least privilege.

NA	OK	NR	***Release Cleanup and Readiness***
	X		Remove any test accounts and/or data, User IDs, and passwords
	X		Remove any unnecessary services, daemons, protocols and/or verify secure use

NA	OK	NR	***Vulnerability Assessment***
	X		Verify use of secure deprecated header files/, API's and functions
	X		Verify Microsoft library components for updated release(s) and vulnerability issues
	X		Verify any third party components for updated release(s) and vulnerability issues

Reviewers Notes: