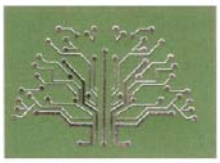

FREEMAN, CRAFT, MCGREGOR GROUP

Source Code Review—Supplemental

Results of regression testing through static code analysis of an updated Technical Data Package (TDP) provided after the initial evaluation, supplemental to *Source Code Review, Verity Voting System 3.0*

Verity Voting System 3.0.1

Report Date: 2018-09-05

Version: 1.1

Status: FINAL

Classification: atsec/FCMG Public

atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
Tel: +1 512 615 7300
Fax: +1 512 615 7301
www.atsec.com

Revision history

Version	Change date	Author(s)	Changes to previous version
1.0	2018-08-27	Ryan Hill	Initial draft
1.1	2018-09-05	Ryan Hill	Updated with client changes

Trademarks

1 Purpose

This report was prepared by atsec information security corporation to review aspects of the security and integrity of the Verity Voting System v. 3.0.1 atsec is an independent, third-party company providing information-security assurance related services.

This report is supplemental to *Source Code Review, Verity Voting System 3.0* and consists of results of regression testing through static code analysis of an updated Technical Data Package (TDP) provided after the initial evaluation.

2 Regression Test Results

Table 1 summarizes the findings that arose from the source code review team's assessment of the updated TDP including code and documentation.

Original Finding Description	Fix Reported by Developer	Regression Test Findings
Password information is not being stored using an appropriate/ suitable class. The class String was being used for passwords.	Use SecureString instead of String.	The modules listed in the work paper were indeed corrected to use SecureString for the password.
SHA-1 was used for sign-hash and sign-data functions which is not supported for FIPS 140-2	Use SHA-256 for the sign-hash and sign-data functions.	The functions mentioned in the work paper were indeed fixed to use SHA-256 instead of SHA-1.
The reviewer was unable to determine how keys and IVs are generated. It was not clear how the keys were generated or how the IVs for the keys were generated.	Update the “Technical Data Package” (TDP) with an explanation of how these are generated.	The TDP was properly updated to address the issue.
Usage of authorized check for a plugin could allow unauthorized use of the plugin and manipulation by an unauthorized user. There was a code authorization function in which it did nothing but return.	Remove the file with no-op function since it was deprecated and no longer used.	The module had indeed been removed.
The SQL query strings were constructed in a way that does not follow best practices and is vulnerable to SQL injection. A bad coding practice of not using parameterized queries was	Change the code to parameterize the query parameters.	The code addressed in the finding had been corrected to parameterize the parameters to the query function.

Original Finding Description	Fix Reported by Developer	Regression Test Findings
being used.		
It was unclear how configuration files were protected from unauthorized modifications. Some information on access was extrapolated from the Technical Data Package.	Update TDP with the appropriate information.	The Technical Data Package was updated with information on using file encryption software to help increase configuration file security by encrypting the drive (which is where the configuration files are located). Using a Trusted Platform Module (TPM) only authentication model, only the person or people with the right credentials (passwords or USB fobs) can unencrypt the drive at boot time.
During the installation of Service Pack 1 (SP1), an installation failure can occur where some updates may not get installed. Some examples of the failed updates include KB2949927 (Availability of SHA-2 Hashing Algorithm) and KB3033929 (Security Update for Windows 7). The software documentation did not contain details on how it addressed this issue.	Update the TDP with the appropriate information.	The developer added a detailed list of Service Packs and other fixes that should be applied to the system to the Technical Data Package (which includes the aforementioned fixes). Using this list, a user can determine if the appropriate fixes were applied to the system.
Microsoft SQL Server 2012 (MSSQL) is not patched.	atsec reviewed Verity_SQL Server 2012 Security Updates Risk Analysis dated July 20th, 2018, provided by the vendor summarizing the known open vulnerabilities in SQL Server and assessing the risk of each to the product.	atsec agrees with the vendor's assessment that because all the currently known vulnerabilities require either remote authenticated user access or cross-site scripting in a browser to be exploitable, a product deployed in the

Original Finding Description	Fix Reported by Developer	Regression Test Findings
	atsec performed a similar vulnerability search and confirmed the vendor's open vulnerability findings.	field and configured properly will not be susceptible to any of these known open vulnerabilities. atsec agrees that having not patched SQL Server currently results in no additional vulnerability to the product.
Use of SHA-1 to sign hashed data.	Moving from the use of SHA-1 to SHA-2.	The vendor has updated the code to use SHA-2 instead of SHA-1 per the NIST requirement.
The product is no longer FIPS 140-2 certified or compliant as claimed.	None	The third-party cryptographic module used by the product has an expired FIPS 140-2 certificate. Unless the provider of the cryptographic module performs such a certification the only resolution is to use another cryptographic module, that is FIPS 140-2 certified as a COTS component in this product. Note that FIPS 140-2 conformance is not the same as the pre-requisite CAVS certificates for the security functions used by the module, but includes conformance with many other requirements such as interfaces, self-tests, design assurance, and key management.

Table 1: Summary of Regression Testing Findings

References

Documentation provided for the regression testing included updated Verity EVS product documentation.

Verity Documents

Change Notes Verity Voting Version 3.0, August 15, 2018

Verity California Use Procedures – Modified Opening Section, August 3, 2018

Workstation WES7 Creation Process Document, August 5, 2018

Verity 3.0 Workstation Configuration Process Document, August 3, 2018

Verity Key Design Technical Document, July 31, 2018

Verity Voting 3.0 Notice of Protected Information, August 6, 2018

Verity_SQL Server 2012 Security Updates Risk Analysis, July 20th, 2018

HP Z240 Verity Workstation Manufacturing Process Document, July 31, 2018