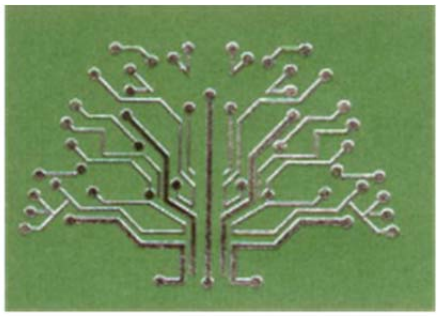
8/28/2017

Security Test Report

ES&S Electionware 5.2.1.0



FREEMAN, CRAFT, MCGREGOR GROUP

COHERENT CYBER

CONFIDENTIALITY NOTICE: This document's data classification is governed by the ISO/IEC 27001:2005 information security classification standards and is classified **PUBLIC.**

Table of Contents

Executive Summary

From May 22 to June 9, 2017, Coherent Cyber, LLC, a subcontractor under the Freeman, Craft McGregor Group (FCMG), conducted a security audit and penetration test or "red team" assessment on the Election Systems and Software (ES&S) *EVS 5.2.1.0 electronic* voting system and all respective components listed under California SOS Contract #16S52058.

The purpose of the assessment was to discover physical and logical security vulnerabilities within the Electionware system that could result in compromising the confidentiality, integrity or availability of voter information or an ongoing election. The team's goal was to enumerate the vulnerability, leverage it to gain unauthorized access to the system, escalate privileges (if necessary) and gain access to vital components within the Electionware suite in order to compromise voter information or change the outcome of an election. The team also validated ES&S's system configurations and hardening procedures in accordance with U.S. federal information assurance guidelines.

Most of the physical security findings involved successfully picking locks common across all devices and removing adhesive based integrity stickers from plastic cases without triggering the tamper safeguard.

The operating system in both the server and the clients had multiple missing patches, including one that fixes the vulnerability leveraged by the WannaCry ransomware. All systems also had multiple misconfigurations based on the DISA STIG and NIST USGCB federal information assurance baselining guidelines.

Multiple vulnerabilities were identified, tested and verified across the server and clients, ExpressVote, DS200 and DS850. Vulnerabilities on the server and clients include default credentials or configurations on out-of-band (outside of the operating system) remote management software. Furthermore, an "unquoted service path" vulnerability was exploited to perform a username and password hash dump from the Electionware database server.

At present, the ExpressVote, DS200, and DS850 do not employ full disk encryption on the primary storage device (i.e. compact flash card or USB protocol-based storage media). This allows an attacker to peer into the file system and reverse engineer all operating system configurations and Electionware software. An analyst was able to make a copy of the DS200 Electionware software, decompile all binaries into human-readable code, introduce a Proof-of-Exploitation code, recompile the source and introduce the modified version of the software back into the system. This code was, in fact, run without evidence of any tampering and cleared all cast votes once the “Close Poll” button was pushed.

Introduction

This document describes Coherent Cyber, LLC, a subcontractor under the Freeman, Craft McGregor Group (FCMG), information security's methodology to conduct the "Red Team Review / System Vulnerability / System Penetration Testing" and review of the **ES&S Electionware 5.2.1.0 Electronic Voting System** ("the voting system" or simply "the system").

Coherent Cyber conducted a hands-on evaluation of the confidentiality, integrity and availability of all physical and logical systems within the voting system. This is to identify any vulnerabilities that could be exploited to:

- alter vote recording
- alter vote results
- alter critical data (such as audit logs)
- conduct a "denial of service" attack on the voting system

This evaluation provided working papers for any vulnerabilities discovered by the analysts and an overall security assessment of the system based on NIST[1] 800-30: *Risk Management Guide for Information Technology Systems* and 800-60 Volume I: *Guide for Mapping Types of Information and Information Systems and Security Categories.* Physical security testing, tamper evidence and detection testing was conducted in accordance with FIPS[2] 140-2: *Security Requirements for Cryptographic Modules*.

The assessment documented and categorized actual or potential vulnerabilities, including any tampering or errors that could cause votes to be incorrectly recorded, tabulated, tallied or reported or that could alter critical election data such as election definition or system audit data.

During the review, the "Red Team":

- Audited configurations and operating system hardening procedures in accordance with industry standard practices
- Audited security and data protection and integrity mechanisms developed or implemented by the vendor (e.g. cryptographic modules)
- Assessed potential vulnerabilities within each system and all networks to which it may be connected
- Provided proof of concept examples of exploitation for vulnerabilities categorized as: "critical" or "high"
- Assessed system audit functions for faults or flaws that may lead to potentially suppressing evidence of a compromised election
- Leveraged the source code review to develop potential exploits within the system

[1] National Institute of Standards and Technology
[2] Federal Information Processing Standards

Testing Methodology

This evaluation provides an overall security assessment of the system based on NIST 800-30: *Risk Management Guide for Information Technology Systems* and 800-60 Volume I: *Guide for Mapping Types of Information and Information Systems and Security Categories.* Physical security testing, tamper evidence and detection testing was conducted in accordance with FIPS 140-2: *Security Requirements for Cryptographic Modules*.

Each vulnerability will be assessed based on the:

- Potential attacker and their level of system knowledge
- Potential loss of election / voter
    - Confidentiality
    - Integrity
    - Availability
- Likelihood of exploitation

Systems Evaluated

The following are the proprietary hardware and software components within the system. All installed operating systems, firmware, vendor software, third-party software, configurations and required hardware devices are implied:

Hardware

Component	Hardware Version	Software Version
ExpressVote	n/a	1.4.10
DS200 Precinct Tabulator	1.3	2.12.1.0
AutoMARK	n/a	1.8.6.0
DS850 Central Tabulator	1	2.10.1.0
ExpressVote Activation Card Printer	n/a	n/a

Software

Component	Software Version
Electionware	4.7.1.0
Event Log Service	1.5.5.0
Removable Media Service	1.4.5.0
Election Reporting Manager	8.12.1.0
VAT Previewer	1.8.6.0
ExpressVote Previewer	1.4.1.0
ExpressPass	n/a
ExpressLink	1.3.0.0
PaperBallot	4.6.1.0

Considerations and Assumptions

All of the systems configured for the assessment were considered properly configured and hardened according to ES&S guidelines. It was further assumed that all software patches and updates were applied prior to the assessment.

It was also assumed that all USB and flash media were wiped prior to creating ballots, transferring election data, and uploading it to the ERM system(s).

Furthermore, the assessment was conducted with the understanding that all polling station equipment, including the ExpressVote and DS200, are not connected to each other, a network, or the Internet via a physical Ethernet connection, radio, telephone line, etc.

Finally, it was assumed that Electionware servers and workstations are connected to an internal network that does not have a route to the Internet or any other unsecured network. Election Management Systems are also assumed to be within a secured facility.

Initial Observations

Electionware Clients and Servers

Dell OptiPlex 5040 workstations are used for the Electionware client software. These systems were loaded with Microsoft Windows 7 Professional x64 edition and commercial anti-virus software. Virus definitions were more than 30 days old since the system does not connect to the Internet. The systems can be configured into one of the following configurations:

Server / Client Configuration – this is used in a medium to large jurisdictions where multiple systems need access to election data and reporting.

Standalone Configuration – this is used in smaller jurisdictions where election data and reporting can occur on the same system.

ERM Configuration – this is used for jurisdictions that only require Electionware to report election data.

Electionware server software is installed on one of two models of Dell PowerEdge servers: T430 or T630. Analysts were informed that, due to their increased processing speed and storage capacity, larger jurisdictions utilize the T630 servers.

DS200 and DS850

The DS200 and DS850 are newer ballot counting devices with modern displays. Each uses USB flash drives to prepare the system to receive and count ballots. The DS200 is installed on a hard-plastic ballot receiver. The DS850 is a high-speed central count digital scanner.

AutoMARK

The AutoMARK is a legacy ballot-marking device used for those voters that fall under the American Disabilities Act and require further assistance to cast a ballot. It has a larger portrait oriented display and uses a compact flash card to load the election on the machine. Due to the limited use of this device, the AutoMARK was not strenuously tested.

ExpressVote

The ExpressVote is the newest ballot-marking device in the Electionware suite and is considered the successor to the AutoMARK. The ExpressVote takes a pre-coded or blank ballot and records all selections made by the voter. This device does not tally votes internally or to external media. An electronic image of the ballot is displayed on the screen for voter verification then printed. The voter will take this ballot and insert it into a ballot box or the DS200 for tabulation. The ExpressVote also uses a Quick Response or "QR" code reader to load a preconfigured ballot and voter ballot choices using the "ExpressPass" functionality.

Findings

All of the assessment findings are divided between three functional groups: physical security, information assurance compliance, and penetration assessment.

Physical Security

There were several physical security vulnerabilities discovered on all of the scanners as well as the AutoMARK ballot marker. These vulnerabilities include:

- Easily picked security locks
- The level of effort needed to compromise integrity seals was easy to moderate
- Integrity stickers were removed from plastic cases without triggering integrity safeguard
- Access to ballot boxes with wire seals in place

Every integrity seal, and all but one of the locks (the double-sided locks on the DS850), are vulnerable to straightforward attacks. In addition, the tamper evidence labels can be removed without triggering the tamper safeguards if they are applied to plastic surfaces.

Another exploit on the DS850 revealed that a thin, stiff probe can be inserted through a gap in the door hinge, allowing the power switch to be activated or deactivated by unauthorized personnel.

Information Assurance Compliance

Using the NIST Security Content Automation Protocol (SCAP), all Electionware servers and workstations were scanned for misconfigurations in accordance with US federal IA standards. These standards conform to mitigating known vulnerabilities and hardening target systems on a US government network.

The following table presents a summary of patches missing on the operating system and misconfigurations on each class (workstation or server) of systems in the Electionware suite.

Electionware Servers

Missing Operating System Patches	
Critical	17
Important	49
Moderate	2
Unrated	8

SCAP Misconfigurations	
Windows 2008 R2 STIG[3]	46
Firewall STIG Configuration	3
.NET Framework 4 STIG Configuration	2
Internet Explorer 9 STIG Configuration	13

Electionware Clients

Missing Operating System Patches	
Critical	24
Important	51
Moderate	1
Unrated	9

SCAP Misconfigurations	
Windows 7 STIG	51
Firewall STIG Configuration	3
.NET Framework 4 STIG Configuration	2
Internet Explorer 9 STIG Configuration	3
Windows 7 USGCB[4] **Configuration**	45
Firewall USGCB Configuration	8

[3] Security Technical Implementation Guide (see references)
[4] United States Government Configuration Baseline

Vulnerability Assessment

Remote Management Default Configuration and Vulnerabilities

All Electionware servers utilize a remote management service that is out-of-band to the operating system. This allows administrators to perform actions on the hardware, whether the system is powered on or not. This service typically uses a network interface port that may also be used for production network traffic. This service, specific to Electionware software, had default administrator level credentials installed and allowed an attacker to remotely reboot or power off the system.

All Electionware client hardware has a remote management service built directly into the hardware chipset. By utilizing recently published vulnerabilities, an analyst was able to leverage a flaw within this management service and gain administrator level access to the management console. Using this access, the analyst was able to reboot or shut down the server remotely.

Unencrypted File System on the ExpressVote, DS200, and DS850

Upon investigating the DS200 and DS850 compact flash cards and the ExpressVote USB flash device, it was discovered that the file systems were not encrypted. Analysts were able to successfully read and modify files on the file systems, and then boot modified media within their respective systems without evidence of tampering.

Access to an unencrypted file system allowed the analyst to recover system configuration information and user password hashes. This access also allowed them to modify the boot device. This provided the analyst with the opportunity to run password-cracking software on user hashes and download the software specific to Electionware's operation. Furthermore, an analyst was able to introduce a proof-of-concept service designed to halt the system on startup and shutdown into one of the Linux-based systems. This vulnerability could be leveraged to introduce malicious software into the system and cause adverse effects to an election.

Java Debugger Service Vulnerability

The DS200 currently has a Java Debugger Service running on its network interface card. This service has a vulnerability that allows an attacker to gain remote access to the system with administrator-level privileges. From here, the attacker can modify files, exfiltrate data or change configurations on the system. It should be noted that an attacker must remove the front housing to gain access to the system's network interface card.

Bytecode Decompiled into Human Readable Source

The Electionware software on the DS200 is currently written in a programming language that allows an attacker to successfully decompile the bytecode into human readable source code. An analyst was able to leverage the zero-disk encryption vulnerability to retrieve the compiled binary then use open-source tools to decompile the bytecode. The analyst was further able to introduce a clear tabulation command within one of the poll closing functions as a proof-of-

concept, recompile the code, and update the DS200 platform. The system booted into the modified version of the software and cleared all cast votes once the analyst initialized the close poll function. Given enough time and resources, this proof-of-concept could be leveraged to compromise an election.

Unquoted Service Path Vulnerability

Both the Electionware client and the servers have multiple services with unquoted service paths. This allows an attacker to insert a malicious executable arbitrarily within the direct path of the service, implementing the malware upon service restart or during the system boot process. For example, if the path was:

```
C:\Program Files\My Software\calc.exe
```

The attacker can rename their malware and place it into the following directory:

```
C:\Program Files\My.exe
```

Due to the nature of unquoted service paths, rather than executing the legitimate service, a malicious service will be executed in its place.

Database User Password Hash Dumping

After leveraging the unquoted service path vulnerability, the security analyst obtained administrator-level privileges and performed a password recovery on the Electionware database server. The analyst was able to obtain administrator-level permissions on the database server and successfully perform a user and password hash dump operation. Hashes were run through hash cracking software; however, due to a limitation in hardware, hashes were not cracked before testing was completed.

References

DISA Security Technical Implementation Guide - http://iase.disa.mil/stigs/Pages/index.aspx
Mitre Common Vulnerabilities and Exposures - https://cve.mitre.org/
NIST SP 800-30 *Risk Management Guide for Information Technology Systems* - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
NIST SP 800-60 Vol 1 *Guide for Mapping Types of Information and Information System to Security Categories* - http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf
NIST SCAP - https://scap.nist.gov/
NIST USGCB - https://usgcb.nist.gov/
USCERT National Vulnerability Database - https://web.nvd.nist.gov/
Quick Response Code - https://en.wikipedia.org/wiki/QR_code