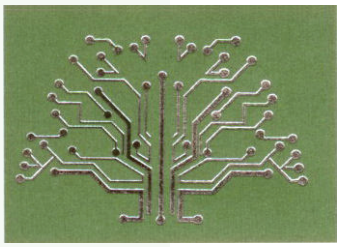

FREEMAN, CRAFT, MCGREGOR GROUP

Vulnerability & Security Assessment Report Election Systems &Software's Unity 3.4.1.0

Prepared for the California Secretary of State by:

Author: Jacob Stauffer, CISSP, FCMG
Contributors: Steve Weingart, CISA, FCMG
William Paine, FCMG

November 4, 2016

Table of Contents

Executive Summary 2

Testing Methodology 5

Systems Evaluated 5

Considerations and Assumptions 6

Initial Observations 6
- **Election Management Systems (Dell Server and Workstation)** 6
- **M100 and M650** 8
- **DS200 and DS850** 10
- **AutoMARK** 11

Findings (Physical Security) 11

Findings (Vulnerability Assessment) 11
- **Federal Information Assurance Compliance** 11
- **Kernel Vulnerabilities in the DS200 and DS850** 12
- **Memory Imaging of DS200 and DS850** 13
- **DS200 Unencrypted File System** 13
- **DS200 Network Configuration** 14
- **DS200 USB Media Not Wiped Before Use** 14
- **Access to Raw Ballot Data (DS200)** 15

References 15

Executive Summary

During the period from May 9 to May 13, 2016, FCMG analysts conducted a vulnerability assessment (red team) on the Election Systems & Software's Unity 3.4.1.0 electronic voting system and all its components.

Throughout the assessment analysts were tasked with discovering physical and logical security vulnerabilities within the Unity system that could result in compromising the confidentiality, integrity, and/or availability of the system. Furthermore, the team tested ES&S' proposed system configurations and hardening procedures in accordance with federal information assurance guidelines specified by the National Institute of Standards and Technology (NIST).

Analysts used the NIST Security Content Automation Protocol (SCAP) to test system-hardening procedures on the Unity server and workstations. The analysts found 269 misconfigurations on the server and 303 misconfigurations on the client standalone and the ERM workstations, as well as multiple security patches that were missing from all systems. These misconfigurations include, but are not limited to, system auditing, password policies, firewall configurations, etc. Furthermore, upon investigating the Linux operating systems found in the DS200 and DS850, analysts found that the target kernel versions had multiple vulnerabilities according to the national vulnerability database. The DS850 system contained at least seven vulnerabilities with the highest criticality score (10) while the DS200 had two.

Physical security evaluations discovered that wire seals used to preserve the integrity of the election could be modified to open and close with little to no visible damage to the outer casing. This makes it possible to open ballot boxes, access compact flash card doors, or obtain printer access. Flat key locks, with the

exception of the double-sided locks on the DS850, were easily opened with a cheap lock picking set obtained through an Internet vendor. Finally, it was discovered that the integrity stickers supplied for the assessment were easily removed from plastic cases without triggering the integrity safeguards. However, testing on metal cases failed and triggered the safeguard on each attempt.

The analysts discovered that the DS200 and DS850 run a custom version of the Linux operating system and represent the newest devices in the Unity system, whereas the M100 and M650 run custom firmware and use external media with non-standard file systems (i.e. FAT or NTFS). Given the scope and time allotted for this assessment, the fact that the M100 and M650 were previously assessed and that the DS200 and DS850 were new to the Unity suite; the DS200 and DS850 were the team's primary focus

During the assessment of both the DS200 and DS850 primary storage devices (e.g. compact flash card, hard drive), analysts discovered that the file systems are not encrypted and allowed the team to recover system configuration information, password hashes, and ES&S specific binaries. It was later discovered that the DS850 performs an integrity check that prevents the system from booting from a modified boot device; however, the DS200 does not perform these checks. Upon further investigation of the DS200, a weak root password hash was discovered, along with an SSH server that allows root logins as well as the ability to trivially image system memory [RAM]. This could ultimately lead to a malicious actor obtaining a DS200 compact flash card, modifying the operating system's configuration and putting a modified operating system into production unbeknownst to election officials or the voter.

Finally, analysts discovered that, once an election is complete, election result tallies are appended to the original election definition file, unencrypted, and written back to the USB media. Investigators were able to find these values from a test election

and attempted to modify the election. A CRC checksum prevented the importing of the modified election into the Election Reporting Manager (ERM). Investigators spent a short amount of time attempting to reverse engineer the file format without success; however, with proper resources, the checksum value could be found and modified to allow importing a modified election; as long as no other countermeasures are in place.

Furthermore, along with the result tallies, the DS200 uploads the full ballot images to the USB media, unencrypted and without file integrity mechanisms (i.e. MD5 or HMACs); to prevent ballot manipulation. It was reported that these ballot images are used to audit the election and, from what the investigators observed, the ERM does not re-tally the election based on these ballots. The investigators were able to modify these ballot images and replace the originals on the USB media without triggering any countermeasures or integrity checking within ERM. This operation could lead to a delay in the election process if the scanned ballots were to be audited.

Testing Methodology

FCMG's approach is primarily geared toward enumerating system misconfigurations and vulnerabilities based on federal Information Assurance (IA) guidelines and computer/network security research. FCMG analysts collect system configurations, vulnerability data and evidence of exploitation of known vulnerabilities. Testing methodologies are 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.* These focus on:

- System characterization / information classification
- Threat source identification
- Vulnerability identification
- Control analysis
- Likelihood of attack
- Impact analysis

Source data for misconfigurations and vulnerabilities include but are not limited to:

- Configurations
  - DISA Security Technical Implementation Guide
  - NIST United States Government Configuration Baseline
- Vulnerabilities
  - NIST National Vulnerability Database
  - MITRE Common Vulnerabilities and Exposures

Systems Evaluated

The scope of the vulnerability assessment covered the ES&S Unity 3.4.1.0 Voting System and included the following components:

- Election Management System (EMS)
  - Audit Manager version 7.5.2.0
  - Election Data Manager (EDM) version 7.8.20
  - ES&S Ballot Image Manager version 7.7.20
  - Hardware Programming Manager (HPM) version 5.9.0.0
  - Election Reporting Manager (ERM) version 7.9.0.0
  - Log Monitor Service version 1.1.0.0

- Hardware
  - DS200 Precinct Scanner HW 1.3/FW 1.7.0.0
  - M100 Precinct Counter HW 1.3/FW 5.4.4.5
  - DS850 – Central Count Scanner
  - M650 Central Ballot Counter HW 1.2/FW 2.2.2.0

- AutoMARK – Polling Place Device various versions
- Dell PowerEdge T430 – EMS Server
- Dell OptiPlex 7020 – EMS Client and Standalone System

Considerations and Assumptions

All systems were considered properly configured and hardened according to ES&S guidelines for the assessment. Furthermore, it was assumed that all ES&S recommended software patches and updates were applied prior to the assessment.

It was also assumed that all USB and flash media were wiped prior to ballot creation, transfer, and uploading of election data to the ERM system(s).

Furthermore, all polling place devices (i.e., the M100 and DS200 precinct count optical scanners and the AutoMARK ballot marking device) are not connected to each other, to a network or to the Internet in any manner. (e.g., an Ethernet connection, radio, telephone line etc.)

Finally, it was assumed that while implemented in an official capacity (e.g. election), EMS servers and workstations are connected to an internal network that does not have a route to the Internet or any other unsecured network. EMS systems are also assumed to be within a secured facility.

Initial Observations

Election Management Systems (Dell Server and Workstation)

The Dell server is a Windows-based server configured as a file server with the purpose to store and share the election data of Unity workstations. No ES&S Unity software was installed on this system. Workstations are Windows based with the Unity software installed and come in one of three configurations:

Server / Client Configuration – used in a medium to large deployment where multiple workstations need access to election data and reporting.

Standalone Configuration – used in smaller deployments where election data and reporting can occur on the same workstation.

ERM Only Configuration – used for deployments that only require the reporting of election data, commonly used to display updated election totals as ballots are being tabulated.

Analysts found that all three configurations (as described above) provided to the red team were missing multiple Microsoft Windows security updates. Furthermore, antivirus definitions were from January 1, 2014.

Figure 1 - Unity Server

Figure 2 - Unity Workstation

M100 and M650

The M100 and M650 are legacy ballot counters within the Unity suite.. The M100 is installed on top of a metallic ballot box and uses a PCMCIA card to setup the system to receive and count ballots.

Figure 3- M100 w/ Ballot Box (Top View)

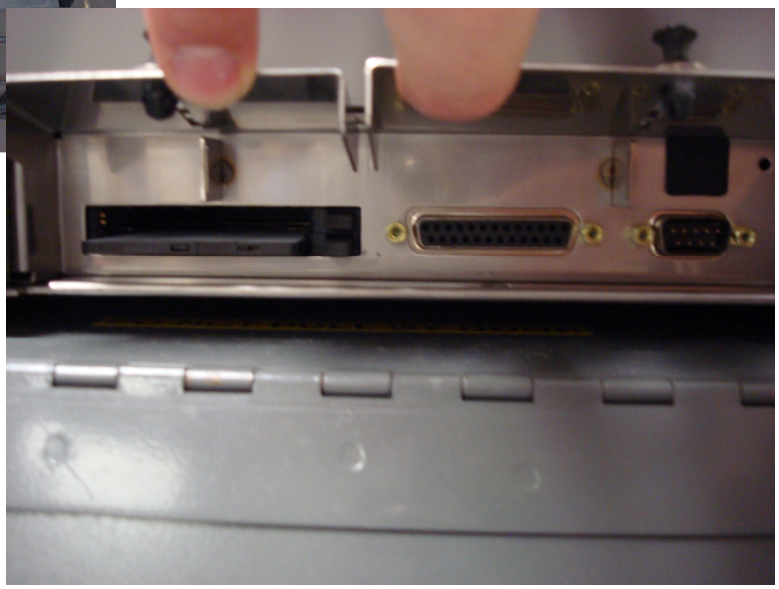

Figure 4 - M100 PCMCIA Slot

The M650 is a central ballot counting device and uses a 250 MB Zip Disk to set up the system to receive and count ballots.

Figure 5 - M650 (Front View)

Figure 6 - M650 Operating Panel

Upon initial investigation of the M100 and M650, it appeared that all parts are of custom design, without commercial off the shelf (COTS) components. Furthermore, the devices are not networked and employ custom operating systems.

DS200 and DS850

The DS200 and DS850 are newer ballot counting devices with modern touch-screen displays, compared to the LCD 7-segment displays on the M100 and M650, and use USB flash drives to update, setup elections and transfer election results to the Unity server/workstations. The DS200 is designed to be installed on a hard plastic ballot box. The DS850 is a high-speed digital scanner that would be used for central volume tabulation of ballots.

Figure 7 - DS200 w/ Ballot Box

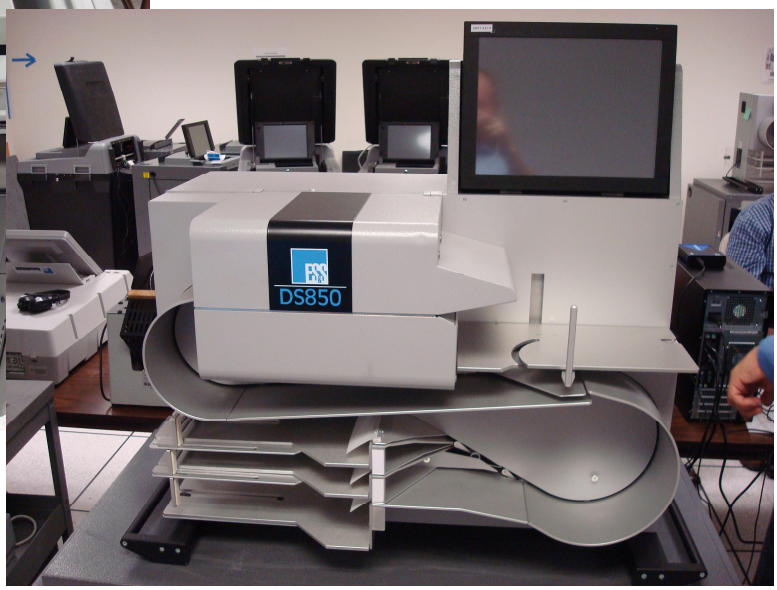

Figure 8 - DS850 (Front View)

Upon initial investigation of the DS200 and DS850, it appeared that most internal parts are COTS and similar to modern computer parts (i.e. CPU, RAM, hard drive). Furthermore, both systems boot a custom version of a Linux distribution as their operating system.

AutoMARK

The AutoMARK Voter Assist Terminal is a ballot marking and verification device providing an independent means of voting for disabled voters in compliance with the Help America Vote Act (HAVA). It has a larger portrait-oriented display and uses a compact flash card to load the election definition onto the device. Nearly identical versions of the device[1] have been subjected to prior security examinations, and the devices typically have limited use, therefore the AutoMARK was not strenuously tested for vulnerability in this examination.

Findings (Physical Security)

Several physical security vulnerabilities were discovered on all of the scanners as well as the AutoMARK . These vulnerabilities included:

- Easily picked security locks
- Easy to moderate ability to compromise integrity seals
- Ability to remove tamper-evident seals (stickers) from plastic cases without triggering the integrity safeguard and
- Capability to access the ballot box without disturbing the wire seals in place.

Testing determined:

1. All locks, except the double-sided locks on the DS850, were easily picked with commonly available tools.
2. Tamper-evident seals could be easily defeated (i.e. removed and replaced without detection) when placed on plastic surfaces.

An additional vulnerability on the DS850 was found when the investigator inserted a thin stiff probe through the door hinge gap allowing access to the power switch. This would allow unauthorized personnel to shut down the system without needing a key or proper access.

Findings (Vulnerability Assessment)

Federal Information Assurance Compliance

Using the NIST SCAP, the Unity server and workstations were scanned for misconfigurations according to federal (IA) standards. These standards provide requirements for identifying, mitigating, and hardening against known vulnerabilities on target systems connected to a US government network. NIST

[1] Prior certified versions included AutoMARK A100 HW1.0/FW 1.1.2258 and A200 HW 1.1 and 1.2/FW 1.1.2258. These same hardware versions are included with new firmware version 1.3.2907 which offered improvements to code quality and minor changes to functionality. New hardware versions Model A200 HW 1.3 and 1.3.1 were include minor design modifications. None of the changes appeared to mitigate risks addressed in prior examinations or to introduce new risks.

recommends voluntary adoption of the standards and use of SCAP for non-federal agencies and for non-governmental organizations.

The following represents a summary of misconfigurations found on the Unity computers that were examined. As a note, the Unity client workstation, the standalone system workstation and ERM reporting workstation were found to have the same general operating system configuration and have been merged as one finding:

Unity Server

- Windows 2008 R2 OS: **131**
- Firewall Configuration: **12**
- .NET Framework 4 Configuration: **5**
- Internet Explorer 9 Configuration: **121**

Unity Client / Standalone / ERM Workstation

- Windows 7 OS: **155**
- Firewall Configuration: **20**
- .NET Framework 4 Configuration: **4**
- Internet Explorer 9 Configuration: **124**

Kernel Vulnerabilities in the DS200 and DS850

The kernel is the most trusted component of an operating system. The exploitation of kernel level vulnerabilities often results in administrator or root level access to the system. These vulnerabilities represent a threat to a Linux system running the target kernel.

Upon analysis of the custom Linux operating system for the DS200 and DS850, analysts discovered that the target Linux kernels versions, recovered from the system's file system, have multiple vulnerabilities. The investigator used www.cvedetails.com to enumerate vulnerabilities specific to the target Linux kernel. It should be noted that none of the vulnerabilities were actively tested during the on-site test. The following is a summary of the findings and their CVSS score [2] according to the national vulnerability database:

[2] Common Vulnerability Scoring System (CVSS) scores vulnerabilities based on their characteristics and impact on a scale from 0 (least criticality) to 10 (highest criticality)

DS850

Score 10	7
Score 9	1
Score 8	2
Score 7	40

DS200

Score 10	2
Score 9	0
Score 8	0
Score 7	9
Score 6	2
Score 5	5
Score 4	19
Score 3	1
Score 2	4

Memory Imaging of DS200 and DS850

The version of the Linux operating system on the DS200 and DS850 systems allows trivial memory imaging. If an attacker was able to access the system, they could use binaries from the operating system to obtain a complete memory [RAM] image.

While this not considered a serious vulnerability, it does allow an attacker to attempt to recover encryption keys, passwords, and other vital system runtime information.

DS200 Unencrypted File System

A file system governs where, how, and who accesses files on a storage device. Typically the operating system governs user access to protected files; however, if the storage device is removed and mounted to another system, access to protected files is possible. Typically, systems that have limited physical security (i.e. mobile devices) encrypt the file system to protect user and operating system files.

Upon examination of the DS200 and DS850 compact flash cards, analysts determined that the file systems were not encrypted. While the DS850 did not allow the system to boot into a modified version of the compact flash card, the DS200 did.

Access to an unencrypted file system allowed the analyst to recover system configuration information, user password hashes and the ability to modify the boot device. Since the analyst was able to modify the DS200's boot loader and gain

console access to the system via single user mode, the next focus was gaining access via the SSH[3] server.

Once the user password hashes were recovered from the system, they were run through a specialized password cracking system using graphics cards. The root password hash was cracked within 46 seconds using a common dictionary attack. The password was confirmed by successfully logging into the SSH server from a remote system. From here, the analyst used this to successfully gain access to an unmodified DS200 within the lab environment.

DS200 Network Configuration

Even though the DS200's Ethernet port is located within the enclosure and not accessible, it is still active by default and configured with a static IP address. Furthermore, it was discovered that an SSH server is installed, which allows remote access with "root" user logins/permissions. Since there is no way to physically login to the Linux operating system when the system is powered on, an actor would need to remotely access the system. Depending on the user's permission, if an attacker were able to access this internal networking port, they would be able to log into the DS200 and access the Linux operating system. Furthermore, as noted in the previous section, the root password was trivially cracked and could be used to gain root-level access to the system.

DS200 USB Media Not Wiped Before Use

Currently the Hardware Programming Module (HPM) does not sanitize or wipe DS200 USB media prior to loading election definitions.

One of the ways to update the DS200 firmware is to write an updater image to the USB media and allow the DS200 to boot from that media. During a test that involved loading an election definition to the device, an analyst wrote the election definitions to a USB device that had updater image installed and rebooted the system with the media installed. Instead of the DS200 booting into the required operating system and loading the election definitions, the device booted the updater image.

This proves that an attacker could build their own custom bootable operating system or malware, write it to the USB devices, have the election definitions written to the devices and boot the systems into the USB media. This action does require the manipulation of the bootloader or a change to the configuration of the DS200 operating system to execute files on the USB media. See the sections regarding unencrypted files systems and network configuration for more information on these modifications.

---

[3] SSH Server – Secured Shell Remote Access Server

Access to Raw Ballot Data (DS200)

After the polls are closed for an election, the DS200 will write the election result tallies to the original election definition file and transfer all ballot images to the external USB flash device. Analysts discovered two findings: the tallies written to the original election definition are in plaintext (unencrypted), and the scanned ballot images are in an unencrypted bitmap format and do not appear to have mechanisms to assure file integrity.

The analysts attempted to modify a test election and import the results into the Electronic Report Manager (ERM). A CRC checksum prevented the importing of modified data into ERM. This would prove that the election results have a cryptographic signature embedded into the file and used for integrity checking. However, due to the unencrypted nature of the data, an attacker could find this checksum value and develop a way to modify the election results and the checksum value, in order to pass as official election results.

Regarding the ballot images, the analysts used common image editing software to modify the bitmap image for a single ballot and save it in the required format. Currently, the ERM does not import these ballot images and re-tally the results. It was reported that these images are used by some jurisdictions to audit the election. With this as fact, an attacker could modify the ballots on the USB media in efforts to bring current election results into question. An election official would have a difficult task to prove that the ballot images were in fact modified without integrity checking mechanisms.

References

CVE Security Vulnerabilities Database – www.cvedetails.com
DISA Security Technical Implementation Guide - http://iase.disa.mil/stigs/Pages/index.aspx
Linux Kernel - https://en.wikipedia.org/wiki/Linux_kernel
Linux Single User Mode - https://en.wikipedia.org/wiki/Single_user_mode
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/
ZIP Disk - https://en.wikipedia.org/wiki/Zip_drive