Threat Event	Description	Threat sources	Threat source characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity, Pervasiveness, and Likelihood of Initiated Attack Success	Overall Likelihood	Level of Impact	Risk
			Capability	Intent	Targeting							
Malware inserted into VxSuite source code	Either through hijacking a VotingWorks developer's credentials, or via some other mechanism, malicious source code is inserted into the VotingWorks source code tree	Adversarial Insider: VotingWorks team member who goes rogue	Moderate	Very High	High	Possible	Low – given strong internal team member vetting & high likelihood of detection	no known applicable vulnerabilities. Depends on a breach of an individual's credentials to Github, or a penetration of Github itself that goes undetected.	Very Low – we have strong controls over authentication of developers, digital signatures on code commits, and a code review process that makes it particularly tricky for a single team member to add malicious code without detection.	Very Low	Very High	Low
		Adversarial Outsider: hacker group, nation state	Very High	Very High	Very High	Predicted	Medium – a reasonable attack to attempt by a capable attacker					
Malware inserted into VxSuite official builds	The official build images are modified after they've been certified by the test lab, but before installation on VxSuite hardware.	Adversarial Insider: VotingWorks team member who goes rogue	Moderate	Very High	High	Possible	Medium – this is harder to trace so lower likelihood of detection	no known applicable vulnerabilities. Depends on physical penetration at VotingWorks facilities, or penetration of transfer storage on Amazon S3.	Very Low – through trusted boot and code signing of the entire executable partition, even a successful modification of the build would require re-signing of the codebase. We have strong controls over the signature keys for code.	Very Low	Very High	Low
		Adversarial Outsider: hacker group, nation state	Very High	Very High	Very High	Predicted	Medium – reasonable to attempt but access is harder to obtain to initiate					
Malware added to VxSuite production machine	A built VxSuite machine is modified to include malware that affects its function, possibly in a way that is hard to detect from normal use.	Adversarial Insider: VotingWorks team member who goes rogue	Moderate	Very High	High	Possible	Medium – harder to trace than source code.	no known applicable vulnerabilities	Very Low – through trusted boot, modifications to a VxSuite production machine are very unlikely to be tolerated without preventing startup.	Very Low	High	Low
		Outsider: hacker group, nation state, individual on customer site	Very High	Very High	Very High	Possible	Medium – reasonable for a capable attacker to attempt	no known applicable vulnerabilities				
Tampered hardware into the VotingWorks supply chain	A scanning unit, CPU, screen, USB receptacle, BMD ballot printer/scanner is modified maliciously in the supply chain before it is assembled into a VxSuite machine.	Adversarial Outsider: nation state	Very High	Very High	Very High	Possible	Low – this is a very involved attack with unfavorable prospects	no known applicable vulnerabilities	Low – fairly unlikely given our use of COTS equipment for much of VxSuite. In addition, as we rewrite most drivers as open-source, tampered hardware is likely to only corrupt input and output to the system, which can often be detected in standard testing.	Very Low	Moderate	Very Low
CVRs on portable media modified before tabulation	The USB drive holding CVRs from VxScan or VxCentralScan is modified before loaded into VxAdmin	Adversarial – attacker on site at the election jurisdiction	Moderate	High	Moderate	Possible	Medium – easy for someone to try	no known applicable vulnerabilities	Very Low – thanks to digital signatures on all transferred CVRs, modifications will generally be detected.	Very Low	High	Low
Election configuration modified	The election configuration, provided by VotingWorks to election administrators before logic & accuracy testing, is intercepted and modified before it is loaded into VxAdmin	Adversarial – attacker on site at the election jurisdiction	Moderate	High	Moderate	Possible	Medium –for someone in an election office with the right access, this is easy to try	no known applicable vulnerabilities or predisposing conditions.	Low – thanks to all processing being closely tied to the election hash, which is prominently displayed to election administrators in configuring equipment, any change in the election definition will likely be detected in L&A testing. An adversarial modification could be a little harder to detect, so marking this "low" as opposed to "very low"	Low	Moderate	Low
		Accidental – operator mistake during tabulation				Predicted – operator mistakes happen			Very Low – thanks to all processing being closely tied to the election hash, which is prominently displayed to election administrators in configuring equipment, any change in the election definition will likely be detected in L&A testing.	Very Low		Very Low
Extraneous CVRs added to the count	Additional CVRs are attempted to be loaded into VxAdmin before final tabulation.	Adversarial – attacker on site at the election jurisdiction	Moderate	High	Moderate	Possible	Medium – easy to try	no known applicable vulnerabilities or predisposing conditions.	Very Low – VxSuite is designed to prevent double-counting any single CVR or CVR file. In addition, all tabulated CVR files are listed clearly, and standard ballot accounting is easily reconciled with VxSuite results.	Very Low	High	Low
		Accidental – operator mistake during tabulation				Predicted – operator mistakes happen				Very Low	High	Low
Loss/Malfunction/Destruction of USB drive holding CVRs during election	The USB drive malfunctions in some way during the election.	Adversarial: someone on site	Moderate	Low	Low	Possible	Low – hard to attempt	no known applicable vulnerabilities or predisposing conditions.	Low – this will happen, and VxSuite is designed to recover easily with a spare USB drive, even during a live election.	Low	Low	Very Low
		Structural: USB device fails Environmental: Fire, eartquake, etc.				Expected – failures happen				Moderate	Low	Low
Loss/Malfunction/Destruction of USB drive holding CVRs after	The USB drive malfunctions in some way after polls are	Adversarial: someone on site	Moderate	Low	Low	Possible	Medium – easy to attempt	no known applicable vulnerabilities or	Very Low – this is unlikely to happen precisely after voting and before tabulation, but if it does,	Low	Low	Low

Threat Event	Description	Threat sources	Threat source characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity, Pervasiveness, and Likelihood of Initiated Attack Success	Overall Likelihood	Level of Impact	Risk
			Capability	Intent	Targeting							
USB drive holding CVRs after election but before tabulation	closed but before final tabulation	Structural: USB device fails Environmental: Fire, earthquake, etc.				Expected – failures happen		predisposing conditions.	VxScan and VxCentralScan can easily re-export data on a new USB drive.	Low	Low	Low
Attempt to import test CVRs into live election	CVRs generated during L&A testing are attempted to be imported into VxAdmin for final tabulation of the actual election.	Adversarial: someone trying to modify the count using test ballots	Moderate	Moderate	Moderate	Possible	High – very easy to attempt	no known applicable vulnerabilities or predisposing conditions.	Very Low – VxSuite makes this impossible.	Very Low	High	Low
		Accidental: the test USB drive is left hanging around, and someone tries to dutifully load all CVRs				Expected - mistakes happen						
VxScan or its components are physically disabled	VxScan becomes non-functional because a critical component fails, e.g. the scanning unit, or the screen.	Adversarial: someone on site physically disables / damages the equipment.	Moderate	Moderate	Low	Possible	High – easy to attempt	no known applicable vulnerabilities or predisposing conditions.	Medium – hardware failures happen, and they are always a disruption. VxSuite handles this as best as we know, by making it particularly easy to swap in backup equipment at any stage of the election. Still, this is a disruption worth having top of mind. VxScan, being voter-facing, is the more likely component whose failure is likely to impact the voter flow more than any other. The use of the emergency ballot box is recommended in that situation.	Low	Moderate	Low
		Accidental: equipment dropped or otherwise damaged Structural: internal components fail as they sometimes do Environmental: Fire, earthquake, etc.				Expected – failures happen				Moderate		Moderate
VxCentralScan or its components are physically disabled	VxCentralScan becomes non-functional because a critical component fails, e.g. the laptop or the batch scanner.	Adversarial: someone on site physically disables / damages the equipment.	Moderate	Moderate	Low	Possible	Low – hard to access as this is controlled by election administrators	no known applicable vulnerabilities or predisposing conditions.		Very Low	Low	Low
		Accidental: equipment dropped or otherwise damaged Structural: internal components fail as they sometimes do Environmental: Fire, earthquake, etc.				Expected – failures happen				Low		
VxAdmin or its components are physically disabled	VxAdmin becomes non-functional because a critical component fails, e.g. the laptop.	Adversarial: someone on site physically disables / damages the equipment.	Moderate	Moderate	Low	Possible	Low – hard to access as this is controlled by election administrators	no known applicable vulnerabilities or predisposing conditions.		Very Low	Low	Low
		Accidental: equipment dropped or otherwise damaged Structural: internal components fail as they sometimes do Environmental: Fire, earthquake, etc.				Expected – failures happen				Low		
VxMark or its components are physically disabled	VxMark becomes non-functional because a critical component fails, e.g. the scanner/printer.	Adversarial: someone on site physically disables / damages the equipment.	Moderate	Moderate	Moderate (BMDs may be more likely a target)	Possible	High – easy to attempt and there have been concerns about BMDs expressed by some	no known applicable vulnerabilities or predisposing conditions.		Low	Low	Low
		Accidental: equipment dropped or otherwise damaged Structural: internal components fail as they sometimes do Environmental: Fire, earthquake, etc.				Expected – failures happen				Low		
Write-in adjudication performed incorrectly	Write-ins are adjudicated incorrectly in VxAdmin.	Adversarial: someone on site uses the write-in adjudication function to add votes to their preferred candidate.	Low	Moderate	Moderate	Possible	Low – this is a low-yield attack	no known applicable vulnerabilities or predisposing conditions.	Very Low – VxAdmin is configured to allow projection onto a big screen for public observation. Given this transparency, the likelihood of this attack (or a mistake) happening successfully is very low	Very Low	Moderate	Very Low
		Accidental: someone clicks the wrong buttons by mistake during write-in adjudication				Expected – mistakes happen				Very Low	Moderate	Very Low
Authentication smartcards stolen	Smartcards used on election day are easily missplaced and could be lost or stolen.	Adversarial: someone steals the cards	Low	Moderate	Low	Possible	High – easy to do	no known applicable vulnerabilities or predisposing conditions.	Very Low – auth cards are protected by multi-factor authentication PINs. In addition, election manager and poll worker cards are keyed to a specific election, worthless for a subsequent election.	Very Low	High – if this succeeded, having an adversary with this access would be problematic	Low
		Accidental: cards are left misplaced on election day for someone else to find.				Expected – mistakes happen				Very Low		Low
Dirt or other deposits prevent	Use of wet ink on ballots, or graphite from pencils, or any other obstructing/sticky substances, create a lasting	Adversarial: a grumpy voter scans a ballot they applied sticky glue to beforehand.	Low	Low	Moderate	Possible	High – easy to do	We have data from one real-world situation where particularly wet markers were accidentally used in an election with VotingWorks equipment,	Medium – we have seen this happen, and it is inevitable. We have mitigations in place, notably making it particularly easy to clean		Moderate – this is	

Threat Event	Description	Threat sources	Threat source characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity, Pervasiveness, and Likelihood of Initiated Attack Success	Overall Likelihood	Level of Impact	Risk
			Capability	Intent	Targeting							
Dirt or other deposits prevent proper interpretation of ballots	other obstructing/sticky substances, create a lasting obstruction on internal scanner glass plates that corrupts interpretation of subsequent scanned ballots.	Accidental: a poll worker offers or a voter uses a wet marker by mistake. Environmental: the weather makes the ballot wet, causing ink that was previously dry to smear on the scanner plates				Confirmed – we have seen this happen in one election in the field		causing the failure described in the risk. This is an inherent predisposition when using modern scanning units that squeeze paper through glass plates in order to focus the image capture.	the scanner when it occurs, and using the auxiliary ballot box if needed. However, it is a concern that should remain top of mind for election administrators.	Moderate	disruptive to the voting flow	Moderate
CVRs are extracted prematurely from VxScan	An attacker can open up the poll-worker compartment on VxScan, extract the USB stick, put in a new one, then use a poll worker card to re-sync the CVRs, and then have a fresh copy of all CVRs and ballot images, before the polls are closed. The attacker can then replace the original USB and close the poll worker compartment.	Adversarial: this only happens if an attacker is attempting to extract those CVRs early, it can't happen by accident. The attacker must have access to a poll worker card.	Moderate	Moderate	Moderate	Unlikely – it's conceivable that someone would attack VxScan this way, but the hurdle is appropriately high as the attacker needs the poll worker card, and even then the risk of getting caught is high. In addition, the payoff is low, so it doesn't seem likely or expected.	Low	The specific feature that makes this attack possible is the re-syncing of CVRs that can be inititated when a new USB drive is inserted, though this does still require a poll-worker card	Low – the poll worker compartment is protected by a seal, a poll worker card is needed, and in most states, the VxScans are under close supervision throughout their use.	Low	Low – in the worst case scenario, it is a partial data leak that doesn't affect election integrity	Very Low