WHITE PAPER

Remediation of Vulnerabilities Identified in CDAs

Prepared by the Nuclear Energy Institute
September 2022

Acknowledgements

This document was developed by the Nuclear Energy Institute. NEI acknowledges and appreciates the contributions of NEI members and other organizations in providing input, reviewing, and commenting on the document including

NEI Project Lead:

Rich Mogavero

Technical Lead:

Jerry Mills – Duke Energy

Member Support:

Stephen Flickinger – Constellation

Michael Dack – Constellation

Ryan Moss – South Texas Project

Brian Young – Energy Harbor

Notice

Neither NEI, nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information apparatus, methods, or process disclosed in this report or that such may not infringe privately owned rights.

Executive Summary

The cyber security rule (10CFR73.54) provides requirements for, and licensee Cyber Security Plan provides measures for incident response and recovery from cyber attacks. Typically, this requirement is addressed by mitigating vulnerabilities and restoring affected systems, networks, and/or equipment impacted by cyber attacks. This guidance provides licensees ways to evaluate vulnerability notifications and potential remediation actions including, but not limited to, application of security patches. Furthermore, the guidance assists licensees by determining and documenting the technical basis, justifying that a CDA is adequately protected. Also, licensees can use this guidance to evaluate whether additional measures are needed to mitigate the vulnerability attack pathways.

Table of Contents

1 INTRODUCTION

Appendix A Sections 4.4.2, 4.4.3.2, and 4.9.1 of the licensee Cyber Security Plans (CSP) requires licensees to address ongoing threats and vulnerabilities to critical digital assets. This commitment is met by performing vulnerability assessments or scans, and evaluations to identify applicable corrective actions to mitigate/remediate vulnerabilities while maintaining adequate defense-in-depth and preventing a CDA from becoming compromised or exploited. NEI 08-09, Addendum 5, "Cyber Vulnerability and Risk Management," addressed vulnerability notification scoring, scoping, and assessment considerations. However, this addendum did not completely address acceptable methods to remediate those vulnerabilities.

2 EVALUATION OF ATTACK VECTORS

An *attack vector* reflects the context by which vulnerability exploitation is possible. An attack vector is not a vulnerability, exploit, or malware. Publicly disclosed vulnerabilities are assigned one of four values for attack vector: network, adjacent network, local, and physical. A description of each attack vector metric value can be found in the latest Common Vulnerability Scoring System Specification Document[1].

Vulnerabilities can be exploited, but not attack vectors, or pathways. Attack vector and attack pathway[2] are sometimes used synonymously; however, attack vector is the preferred term because it is the one used by CVSS (Common Vulnerability Scoring System).

A *vulnerability* is a flaw in the design, implementation, or configuration of software that has security implications. Vulnerabilities are classified by their severity (i.e., CVSS base score). CVSS scores are mapped to qualitative ratings of *Critical, High, Medium, Low*, and *None*. To distinguish between different vulnerabilities, they are assigned CVE (Common Vulnerability and Exposure) IDs and might be given a name. For example, *BlueKeep*[3] refers to a specific vulnerability (CVE-2019-0708) in Microsoft's Remote Desktop Protocol (RDP) implementation. This vulnerability is assigned the attack vector metric value of "*Network*" because the vulnerable component is bound to the network stack (RDP listens on port number 3389, by default) and it can be exploited *at the protocol level* one or more network hops away (e.g., across one or more routers). The vulnerability's attack vector is "*Network*", not RDP port 3389.

An *exploit* is a piece of code or a program that takes advantage of a weakness in software or system. Exploits are typically classified by the resulting behavior after a vulnerability is exploited, such as arbitrary code execution, privilege escalation, denial of service, or data exposure. Exploits might sometimes be given a name. For example, *EternalBlue*[4] refers to code written to exploit multiple vulnerabilities in Microsoft's Server Message Block version 1 (SMBv1) protocol. The most severe of the vulnerabilities (i.e., those with a higher CVSS score) could allow *remote code execution* if an attacker sends specially crafted messages to a vulnerable (unpatched) SMBv1 server over a network[5]. The attack

[1] https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf
[2] NRC's definition of attack pathway is derived from the definition of attack vector in SNL technical report SAND2012-2427. Ref.: https://irp.fas.org/eprint/metrics.pdf
[3] https://www.microsoft.com/security/blog/2019/08/08/protect-against-bluekeep/
[4] https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf
[5] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 (Microsoft Security Bulletin MS17-010)

vector of the SMBv1 vulnerabilities *exploitable by EternalBlue* is "*Network*". The exploit is not an attack vector. Attackers or malware, leverage exploits to achieve their end goal.

Malware is classified by the payload or malicious action it performs. Malware must be delivered, for example, across a network or via physical media, to a target system and then executed. For example, *WannaCry*[6] is a specific type of malware (ransomware) that uses the *EternalBlue* exploit to spread itself across a network infecting all connected devices and dropping a crypto-ransomware payload. The attack vector of the *exploited* vulnerability is "*Network*" even if the malware is initially transferred to a system using portable media.

CVSS metrics do not account for threats presented by the supply chain or use of portable media and devices. With respect to these channels, the concern is with introducing, or delivering, "patches, software updates, replacement firmware, replacement hardware/components that contain malicious and/or detrimental elements such as time-bomb logic, unauthorized backdoors, hidden functionality, degraded components, faulty designs, etc., that can adversely impact the functionality of the CDA"[7]. The supply chain, portable media, and devices are an indirect means to introduce malware into a target system; they are not attack vectors from the perspective of vulnerabilities.

App. E Sec. 3.5 requires licensees to "receive security alerts, bulletins, advisories, and directives from credible licensee-designated external organizations on an ongoing basis". Examples of a credible external organization are the U.S. government's Cybersecurity & Infrastructure Security Agency (CISA) and NERC's Electricity Information Sharing and Analysis (E-ISAC).

Security alerts and advisories provide information related to observed threat activity and publicly disclosed vulnerabilities to raise situational awareness regarding new threats, campaigns, and incidents and to notify users about security issues affecting vendor products.

When reviewing alerts and advisories pertaining to specific threats (e.g., malware) or threat activity, licensees should ensure associated vulnerabilities are assessed and addressed.

Consider *SUNBURST backdoor/*SolarWinds[8] supply chain attack. *SUNBURST* is malware, not a vulnerability (*SUNBURST* doesn't have any assigned CVE IDs). A licensee could have unwittingly introduced the backdoor into its plant environment during an install or routine software update. The backdoor would not have been detected by a malware scanning kiosk when scanning the portable media or device used to transfer the compromised software package. Once installed in the environment, remotely accessing the backdoor for command and control purposes is mitigated by the defensive architecture. In addition, a licensee would have been made aware of the presence of the backdoor ~~vector~~ by US-CERT alert AA20-352A[9], E-ISAC Critical Broadcast Program All-Points Bulletin 20-08, and SolarWinds security advisory[10] and taken corrective action.

[6] https://www.cisa.gov/uscert/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf
[7] NRC NSIR Fundamentals Document
[8] https://www.cisa.gov/uscert/ncas/alerts/aa20-352a
[9] https://www.cisa.gov/uscert/ncas/alerts/aa20-352a
[10] https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network

When assessing a vulnerability, the licensee should account for how exploitation is possible (i.e., attack vector) because environmental factors that prevent inbound network traffic such as standalone, or air-gapped, networks or use of data diodes limit an attacker's ability to *remotely* exploit certain types of vulnerabilities or take command and control.

Not all exploits accomplish the same end, and an exploit is not an end in and of themselves, except perhaps as proof of concept; they are a means to end (i.e., used to mount a cyber attack). Ultimately, it's the actions taken by an attacker (or malware) after exploitation occurs, that determines impact to safety, security, and emergency preparedness functions.

2.1 Considerations of The Design Basis Threat

The capabilities of a nation-state actor are "beyond design basis threat."[11] Per the requirements within 10 CFR 73.1, the design basis threat of radiological sabotage includes a cyber attack. A *cyber attack* is a deliberate act directed against a nuclear power plant, specifically, against protected assets (digital systems and networks subject to 10 CFR 73.54) to compromise their security. As stated in 10 CFR73.54 (a), cyber attacks that must be protected against are bounded "up to and including" the design basis threat of radiological sabotage[12]. The cyber security defensive architecture is the primary line of defense against nation-state actors and targeted zero-day vulnerabilities.

3 DETECTION PRIOR TO ADVERSE IMPACT

During vulnerability analysis, the focus is preventing exploitation of a vulnerability that affects detecting the compromise prior to actions being taken to protect the SSEP function or a direct CDA.

Indirect CDAs

NEI 13-10, (Cyber Security Control Assessments) states, "Indirect CDAs are those CDAs that cannot have an adverse impact on Safety or Security functions prior to their compromise or failure being detected and compensatory measures being implemented by a licensee." NEI 13-10 also includes, "impact to Direct CDAs." For indirect CDAs, the licensee must also determine "time to detect".

Vulnerabilities for Indirect CDAs may be evaluated using the same criteria. When it can be shown that a vulnerability does not change the potential impact, time to detect, or compensatory measures, the vulnerability may be considered fully mitigated.

If potential impacts of vulnerabilities can be addressed generically and included in the indirect assessment, then, they need not be considered individually for newly identified vulnerabilities.

When evaluating generic application of mitigations, the following questions and statements should be considered:

- Can detection be compromised?
    - Is detection digital or perhaps human?

[11] 10 CFR 50.13, "Attacks and Destructive Acts by Enemies of the United States; and Defense Activities"
[12] 42 FR 34310 Radiological sabotage is a term used instead of industrial sabotage to more clearly indicate that the sabotage of concern is that with *radiological consequences* (as opposed to vandalism)

    - Is detection dependent on an application such as logging, whitelisting, or virus protection?
- Is the Indirect CDA isolated from Direct CDAs by IPS (intrusion protection system) or Firewalls with protection for the protocols used which can limit spread?
    - Does the firewall or IPS limit the communications to known screen-able protocols?

(Firewalls, IPS, IDS are at least considerations for determining urgency of patching even if they do not provide specific protocol screening)

When evaluating impact for an individual vulnerability, only the following need to be considered:

- If detection depends on software or digital infrastructure, can the vulnerability affect the ability to detect compromise?
    - Is the vulnerability in an application such as logging, whitelisting, or virus protection that is depended on for detection or limit the ability of the CDA to run the detection application?
- Does the vulnerability create an unanalyzed means to attack a Direct CDA?
    - Could this vulnerability evade network protections such as HIDS or NIDS which would prevent or slow attacks or access to a Direct CDA?
    - This is not a consideration for isolated CDAs

4 MAINTAINING DEFENSE IN DEPTH

Maintaining defense-in-depth (DID) is a requirement of a licensee's cyber security plan and was codified by the 2009 Power Reactor Security Requirements rulemaking, 10CFR 73.54(c)(2). The NRC delineated specific requirements during the rulemaking period as to how DID is achieved and to clarify the unique differences with DID for 10CFR 73.54 and 10 CFR 73.55, as well as distinguish DID from the traditional design engineering concept of Nuclear Power Plant (NPP) operations.

…The Commission concluded that defense-in-depth for digital computer and communication systems and networks includes technical and administrative controls that are integrated and used to mitigate threats from identified risks…[13]

The 2009 rulemaking Statements of Consideration provides the DID distinction for Cyber Security as:

[With regard to § 73.54(c)(2),] defense-in-depth for digital computer and communication systems and networks includes technical and administrative controls that are integrated and used to mitigate threats from identified risks. Defense-in-depth is achieved when (1) a layered defensive model exists that allows for detection and containment of non-authorized activities occurring within each layer, (2) each defensive layer is protected from adjacent layers, (3) protection mechanisms used for isolation between layers employ diverse technologies to mitigate common cause failures, (4) the design and configuration of the security architecture and associated countermeasures creates the capability to sufficiently delay the advance of an adversary in order for preplanned response actions to occur, (5) no single points of failure exist within the security strategy or design that would render the entire security

[13] https://www.govinfo.gov/content/pkg/FR-2009-03-27/pdf/E9-6102.pdf

solution invalid or ineffective, and (6) effective disaster recovery capabilities exist for protected systems.

These six (6) points provide the building blocks on how a licensee must ensure identified vulnerabilities are protected from exploits, ultimately impacting an SSEP function. Though 10 CFR 73.54(c)(2) is specific to a NPP's Cyber Security Program, these six points explain that DID has inherent NPP operating principals. These principals indicate a holistic approach to mitigating vulnerabilities. Above, items 1, 2, and 4-6 generate their requirements from already imbedded standards set forth in Operations, Engineering, and Security sectors of NRC Regulation. These standards have built a framework that allows for the Cyber Security Program to fully integrate into DID architecture that protects against exploitable vulnerabilities.

4.1 Technical Controls Considerations for Exploitation

The NRC's first area of Cyber Security DID, *Technical Controls*, provides Licensee's with the ability to implement an effective, wide variety of security controls for the mitigation of risks to digital systems. A security control is applied when there is high assurance that CDA is adequately protected and DID is maintained. Cyber Security Technical Controls are in place to support maintaining DID for identified vulnerabilities. Non-networked equipment or isolated trains of equipment help separate the impact, or even the possibility of impact, to an SSEP function if exploited. These technical controls are tools used across all 6 points above to maintain DID and are, in general, new to the NPP operating standards and policies prior to the 2009 Cyber Rule (See section 4.3 for vulnerability chaining).

4.2 Administrative Controls Use of Restrictions on Logical Access Permissions

The NRC's second area of Cyber Security DID, Administrative Controls, provides Licensees with the ability to credit certain organizational protocols that, from a NPP operator perspective, were already in place prior to the Cyber Rule, as well as the development of new administrative controls described in the cyber plan.

Pre-Cyber Rule administrative security protocols, such as Personnel Security and Access Controls, Physical Environment Protection, Vulnerability Management, Monitoring and Maintenance Programs, Configuration and Change Management Programs, Training, Supply Chain Protection and Periodic Program Health Check Polices are all critical in providing the framework by which DID is achieved. Nuclear Power Plant operators have relied on these programs and policies prior to the Cyber Rule and the effectiveness has proven over time to adequately address risks and threats a NPP may incur.

Post-Cyber Rule Administrative Controls such as Cyber Attack Mitigation and Response, Enhanced System and Information Integrity, Media Protection, and Cyber Recovery Plans build upon the already strong NPP administrative infrastructure to further harden against the Design Basis Threat (DBT). In an operating environment, these administrative controls integrate the technical controls into a systematic approach to DID. The exploitation of a vulnerability is further mitigated using these administrative controls, which stretch beyond the immediate capability of a technical control and provide a broader organizational approach managing vulnerabilities.

4.3 Further Considerations for Vulnerability Chaining

Note
This section is informational on the concept of vulnerability chaining for consideration when chained vulnerabilities have been identified as exploited. This does not change the requirement to address vulnerabilities below a CVSS score of 7.0 for CDAs and a CVSS score of 4.0 for defensive architecture.

CVSS User Guide defines and describes the concept of *vulnerability chaining*[14]. Vulnerability chaining is the sequential exploitation of multiple vulnerabilities to attack an IT system, where one or more exploits at the end of the chain require the successful completion of prior exploits to be exploited. Identified vulnerabilities that, if exploited, could expose, or directly impact another vulnerability, should be evaluated, and analyzed as a singular exploitation impact. Whereas vulnerabilities that have no direct impact to each other may be evaluated individually. Chaining vulnerabilities should be an element of the vulnerability management assessments. A vulnerability should be considered based on its potential as a gateway to a CDA with adjacent vulner4.3abilities to a local attack vector.

If a vulnerability can, be exploited only after other preconditions are met (such as first exploiting another vulnerability), it is acceptable to combine two or more CVSS scores to describe the chain of vulnerabilities by scoring for the least-restrictive Exploitability sub-score metrics and scoring for the most-impactful Impact sub-score metrics.

For example, consider VMware vulnerabilities CVE-2022-22954 (base score 9.8 / network) and CVE-2022-22960 (base score 7.8 / local). According to US-CERT alert AA-22-138B, in one instance an unauthenticated actor with network access to the web interface leveraged CVE-2022-22954 to execute an arbitrary shell command as a VMware user. The actor then exploited CVE-2022-22960 to escalate the user's privileges to root. The chain of these vulnerabilities has a base score of 9.8. In other words, CVE-2022-22954 has the same severity but CVE-2022-22960 is more severe if exploited remotely via chaining than if locally.

4.4 Appropriate Use of Defensive Architecture

Licensees should consider the following points to ensure DID is maintained with justification using technical and administrative controls:

- Applied technical security controls or alternate controls
- Non-networked equipment or isolated trains
- Crediting IPS segmentation when the IPS understands the protocol and the segmentations would preserve the SSEP function from a single cyber attack
- Through analysis or If test systems exist consider penetration testing to show the vulnerabilities are not easily exploitable without external tools or resources
- Physical Security – Protected Area, Vital Areas, Locked Cabinets, Key control program
- Use of Critical Group
- Configuration management
- Work control process
- Centralized / local IDS and log monitoring
- Portable media and device program

[14] https://www.first.org/cvss/v3.1/user-guide

- Incident response and disaster recovery

The technical and administrative controls implemented by a licensee constructs the comprehensive DID strategy achieving the points noted within the NRC's 2009 Security Rule Statements of Consideration. Managing vulnerabilities occur in numerous ways, including patching to mitigate against any exploitation. In some cases, the evaluation may identify a period when patching may not be the primary method to mitigate the vulnerably due to other technical or administrative controls set forth in a station's DID framework. In these cases, it may be the intent to ultimately patch or replace the system however, licensees may decide to continue with the current configuration until there is a more appropriate time of remediation (e.g., refueling outage, maintenance outage or complete modification is implemented). Having such a breadth of DID technical and administrative controls allows Licensees to demonstrate with a high assurance that a vulnerability will not be exploited and adversely impact an SSEP function.

5 EQUIPMENT PAST END OF SUPPORTED LIFE

5.1 Use of Vulnerability Scans and Evaluation of Results

For equipment beyond the vendor's supported life cycle, vulnerability scans may be used to fulfill the CSP and E.12 requirements. NEI 08-09, Rev. 6 states the following:

- Vulnerability assessments or electronic vulnerability scanning of CDAs are performed as described in Appendix E, 12, "Evaluate and Manage Cyber Risk," when new vulnerabilities that could affect the cyber security posture of CDAs are identified.

Control E.12 lists the following requirements for selection of a scan tool:

- Enumerating platforms, software flaws, and improper configurations,
- Formatting and making transparent, checklists and test procedures; and
- Measuring vulnerability impact

Scans must be performed with privileged accounts to ensure thorough scanning. If available, use test or development systems for scanning. If test systems are not available, and scanning is required on production equipment, the 92-day requirement may be extended until the equipment can be taken off-line (i.e., outages). Considerations for analyzing applicability of vulnerabilities from scans.

Vulnerabilities identified from scanning older, out of support software, frequently includes vulnerabilities which have never been exploited. For this software, see section 6.5 for considerations associated with currently exploited vulnerabilities.

5.2 Addressing Known / Unknown Vulnerabilities and End of Life (EOL) Equipment for Direct CDAs

Note:
This section covers Addendum 2, “Cyber Attack Detection, Response, and Elimination” to NEI 08-09 as it is most applicable to Threat and Vulnerability Monitoring (TVM). Refer to Addendum 2 for additional information. See Section 3 for Indirect CDAs

As Stated in Addendum 2 to NEI 08-09, 10 CFR 73.54(e) requires that the cyber security plan must describe how the licensee will:

I. Maintain the capability for timely detection and response to cyber attacks;
II. Mitigate the consequences of cyber attacks;
III. Correct exploited vulnerabilities; and
IV. Restore affected systems, networks, and/or equipment affected by cyber-attacks.

Addendum 2 further states, "the assessment elements in this Addendum would apply to Direct CDAs." and "This document discusses the capability to detect, respond-to, and eliminate (DRE) cyber attacks. In this context, the term ‘eliminate’ is inclusive of concepts of mitigation and prevention of the adverse impacts of a cyber attack." Based on these concepts an acceptable goal of TVM for Direct CDAs, is to detect and mitigate to protect the SSEP function of the direct CDA.

When considering if a licensee has timely detection, the following questions should be asked:

- Did the licensee place its detection capability along the attack pathway(s) at a location where it can detect cyber attacks and permit the licensee to respond and eliminate the cyber attacks before an adverse impact to the SSEP function?
  For TVM IDS or IPS placement, consider:
  - Placement between redundant components
  - Network traffic paths, placed between HMI and Server or IO and server
  - A known protocol (to the IDS\IPS) being used such that it can be effectively be inspected

- Are personnel responsible for cyber attack detection trained in accordance with licensee training standards, and are they sensitive to the indications of a cyber attack?
  - Are responders trained on detection indicators?

- Is there capability for near real time indication of attack?:
  - Is the CDA connected to a SIEM and it is properly configured to alert on attack indicators.
  - Is the IPS/IDS connected to the SIEM.
  - Updating one system at a time with protections between redundant systems can be an indicator for zero-day exploits
  - Is signature-based detection maintained and updated?

When near-real time detection of an event is neither possible nor available, a basis is needed for the potential delay. A Direct CDA is directly performing the SSEP function, therefore time to detect must be

based on a license-based standard such as a Tech Spec surveillance. See NEI 08-09, Addendum 2, Section 3 for use of existing Programs and Processes for non-real time detection methods.

5.3 Credit for Whitelisting

Whitelisting does not remove the vulnerability; however, it addresses the ability to exploit vulnerabilities by accessing the system locally and executing code (or executable scripts). In this case locally refers to where the code must run. It includes remote shell or desktop access. It can be considered as part of the remediation of a network or adjacent vulnerability when other measures address network access.

- Whitelisting addresses local exploits of a vulnerability which cannot be exploited without local code execution.
- Whitelisting does not address vulnerabilities which can be exploited by direct user interaction with the vulnerable code.
    - Consider what other restrictions exist on direct user interaction (i.e., user interface vulnerabilities).
- If the vulnerability is in the OS or existing applications, only LOCAL exploitation aspects are being addressed.
- Network layer vulnerabilities exploited remotely are not addressed by whitelisting.

5.4 Scanning

Most scanning tools categorize discovered vulnerabilities as, **Low** to **Critical**. Sites should use the same criteria as is described in NEI 08-09 Rev. 6, Addendum 5 for determining which vulnerabilities require analysis. Using the NRC approved guidance, Medium for Defensive Architecture and High and above for all other CDAs.

It may not be necessary to fully analyze all vulnerabilities determined to be applicable from a scan. For indirect CDAs, the same processes of Section 3 apply to vulnerabilities identified during a scan.

Additionally, the licensee CSP Control E.12 allows the use of security testing to determine the level of difficulty in circumventing the security control. If security testing has been performed on the system or test system, it can be considered as part of remediation of the vulnerabilities.

5.5 Mitigations for End-of-Life Equipment

Consider the following “Short Term Mitigation Strategies” for bridging time to implement longer term solutions, such as system upgrades or longer-term protections.

- Application of the DRE (Detect, Respond to, Eliminate) processes within this section.
- Credit defense in depth and create additional defense in depth with measures such as additional physical security, increased monitoring, or additional administrative measures (working in pairs with verification).

Below are the longer-term solutions to consider when implementing protections:

- Installing whitelisting products on older systems can typically support current virus protection.
- Adding additional detection, such as custom applications which monitor running processes and send SIEM alerts.
- Add network segmentation such as IPS between redundant systems. If the IPS supports the protocols being used, credit it for protection of the SSEP function against network vulnerabilities.
- Determine if the platform can be upgraded, hardware and OS, without a system upgrade. Current Operating Systems are more versatile in their ability to run applications developed for legacy OS than they used to be.
- Consider emulation tools to allow update of the OS for example, Microsoft created a toolkit to allow Windows CE to run on Windows 10 and 11.

6 IMPLEMENTATION OF REMEDIATION

Remediation is the act of correcting a vulnerability *or* mitigating a threat. Three ways of correcting a vulnerability are installing a patch, adjusting configuration settings, or uninstalling a software application.[15] Threats are mitigated by strategically allocating security controls so that adversaries have to overcome multiple (two or more) safeguards to achieve their objective (i.e., a cyber attack per 10CFR73.1). Requiring adversaries to defeat multiple mechanisms increases "adversary work factor" (makes it more difficult, not impossible, to exploit a vulnerability to compromise the security of a protected asset) and increases the likelihood of detection.[16]

A licensee might be unable to correct a vulnerability for various reasons (e.g., risk of interruption to plant operations, lack of vendor support, end of product lifecycle/obsolescence). In this case, the focus should be on prevention or detection to accomplish threat mitigation.

It is assumed a licensee has already screened vulnerabilities against its inventory of software and hardware in accordance with NEI 08-09, Rev. 6, Addendum 5 guidance to determine whether they are applicable to their environment.

The subsequent assessment may contain the following based on the licensee's Corrective Action Program:

- Document, if applicable, vulnerabilities are exploitable;
- How these vulnerabilities will be corrected, or;
- If not correcting applicable vulnerabilities, identify:
    - Other measures that would prevent vulnerability exploitation
    - Detect attempts to exploit vulnerabilities,
    - Detect exploited vulnerabilities, or;
      Other detect and delay actions taken by attacker after exploitation and document these measures and why they provide adequate defense-in-depth.

Questions to consider:

[15] NIST SP 800-40 Rev. 2.
[16] NIST SP 800-53 Rev. 4

- What attack vectors are applicable in attempting to exploit the vulnerability?

The attack vector value can be easily determined from the CVSS vector string (a text representation of a set of CVSS metrics commonly used to record or transfer CVSS metric information in a concise form). An attack vector reflects the context by which vulnerability exploitation is possible. CVSS identifies four possible values for attack vector: network, adjacent, logical, and physical. A vulnerability is assigned only one of these values.

A license should consider and document where (physically and logically) within its environment an affected component resides and whether the vulnerability can be exploited in its current configuration. Some vulnerabilities might require certain preconditions be met to be exploited. Any preconditions shouldn't be a reason to conclude a vulnerability isn't exploitable but should be used later in the assessment to identify pertinent measures that will prevent or detect a vulnerability from being exploited.

If a remotely exploitable vulnerability (attack vector is "network") affects a critical digital asset connected to an isolated (air-gapped or behind a data diode) network, then a license should consider the attack vector to be "adjacent" (limited at the protocol level to a logically adjacent topology such as a local area network).

If it is determined that a vulnerability is not exploitable, then explain why.

- What security controls are currently in place that protect the CDA from exploitation of the vulnerability as described in the alert or notification document?

If it is determined in the prior question that a vulnerability is exploitable, then identify the safeguards or barriers that must be defeated for an attacker (or malware) to accomplish exploitation.

A licensee should credit any security controls already in place that would prevent or detect an attacker (or malware) attempting to exploit a vulnerability (e.g., unescorted access authorization, behavioral observation program, physical access control, system monitoring, port blockers, control of portable media/file transfers, device whitelisting, security and operator rounds).

For example, assuming a standalone network, an attacker (or malware) would need access to a system's local area network to exploit a network-based vulnerability. To accomplish exploitation, the following barriers would need to be overcome:

  - To access the network, the attacker would need to connect a laptop to a network switch. The network switch is located in a secured location. Port locks are installed on connected network cables plugged into the switch and port blockers are installed in all unused ports. Port security is enabled on interfaces (switch ports) in use and unused interfaces are administratively shutdown. The network is monitored and alerts when a "rogue" system is connected.
  - If a critical digital asset is not connected to a network, then an attacker would be unable to exploit any network-based vulnerabilities (those with the CVSS attack vector of "network" or "adjacent") despite being vulnerable.

Any threat posed by an attacker attempting to remotely exploit a vulnerability from outside of a network's logical and physical confines, is mitigated.

Inadvertent or unintentional conduct such as introduction of malware with or without adverse impact should not constitute a cyber attack.

- How do the existing security controls prevent an attacker (or malware) from exploiting the vulnerability?

Correcting a vulnerability is the best approach to prevent exploitation. Another option to consider is applying a workaround, if available, which usually involves adjusting configuration settings instead of patching. When a licensee is unable to correct a vulnerability, the focus should be on other preventive or detective measures such as intrusion prevention or detection.

A licensee must describe how the safeguards identified in the previous template question prevent or detect attempts to exploit the vulnerability in question in the context by which vulnerability exploitation is possible (i.e., attack vector).

Security controls are safeguards that must be defeated by an attacker (or malware) to have an opportunity to exploit a vulnerability. If multiple (two or more) barriers must be defeated before an attacker could have an opportunity to exploit a vulnerability, then it can be concluded that security controls in place provide adequate defense-in-depth protection despite a critical digital asset still being vulnerable.

- Document recommended short and/or long-term corrective actions to mitigate or remediate the vulnerability when the assessment concludes corrective actions are needed to maintain adequate defense-in-depth.

If a licensee fails to identify security controls in the second question above that would prevent or detect exploitation of the vulnerability (under consideration) or determines they are inadequate, then corrective action must be taken.

If remediation is required because the depth of defense is reduced (inadequate defense-in-depth), then the license should document any corrective actions being taken to remediate the vulnerability. Recall from above, correcting a vulnerability is the best approach to prevent exploitation. Another option to consider is applying a workaround, if available. When unable to correct a vulnerability, the focus should be on other preventive or detective measures.

- Prevention includes any way to eliminate the vulnerability on the CDA (e.g., patch, remove, change configuration, additional barriers targeting vulnerability).

- Detection includes updating and validating attempts at exploitation of the vulnerability would be flagged by anti-virus, software integrity, network detection systems, or other detection systems (e.g., update signatures, apply/enable intrusion detection rules).

When detection is relied upon, it shall be expected that a documented time for prevention would be established. The documentation may be through a business plan, Condition Report action, or another long-range plan identifier to share with stakeholders for the next available opportunity to address prevention of the exploit. This would be a future upgrade, install, or replacement that would eliminate the vulnerability. If no such plan exists, then documenting that no such plan exists should be a part of the assessment and understood by the owners.

7 ADDRESSING TVM WITH VENDORS – PO/SPEC REQUIREMENTS FOR EQUIPMENT UPGRADES

7.1 Evaluating a Vendors TVM program

The NVD (National Vulnerability Database)[17] is the U.S. government repository of standards-based vulnerability management data that can be used to identify vulnerabilities. Utilities use this database as an awareness tool for identifying vulnerabilities and potential impacts to CDA functions and supported equipment within the OT (Operational Technology) environment. While Government Suppliers have begun to understand the importance of vulnerability management programs, many suppliers and system integrators have not. Many control system vendors expect their systems to be isolated or firewall protected and may not patch. Most have a vulnerability management program; however, it may not be adequate in identifying the potential impacts associated with the exploitable vulnerabilities.

To evaluate the adequacy of a proposed vendor program, consider the following questions:

- Who are the system integrator's suppliers? Do the suppliers have a TVM program?
- A TVM evaluation must include every product the vendor installs. Check versions and lifecycle of everything including less obvious products such as backup software which typically runs with high privileges.
- Does the system integrator, including all suppliers report vulnerabilities to NVD?
    - Do CVEs (Common Vulnerabilities and Exposures) have enough information to be scored? (Not just the vendor supplied score)
    - Do the CVEs typically contain work arounds (options other than patching)?
    - Is there enough information supplied for you to evaluate the potential impact to the function vs risk of exploiting the vulnerability?
    - Reporting to NVD isn't enough. Does the vendor and product appear on NVD's CPE (Common Platform Enumeration) list? The CPE list is how a product can be tied to products used or included in the base product.

7.2 Purchase Orders and Specs

System integrators see it as more cost effective to continue to use a platform or OS if possible, rather than absorb the cost of redesign. Because of this, accepting a vendor's "standard product" frequently yields soon to be out of support products

To ensure a PO or Spec contains enough requirements for purchasing a supported product, consider the following:

- Require that all operating systems and installed software shall be within the original suppliers supported life plus no less 3 years.
- Many manufacturers have long term support options. For example, some builds of most Windows products are part of the long-term support channel which guarantees at least a 5 year

[17] https://nvd.nist.gov/

supported life. Depending on where in the windows lifecycle your purchase is, it can be up to 10 years. Request those builds when possible.

- If network equipment is required, ensure the PO requires managed network equipment. Monitoring increasing the case for detection which helps extend the equipment life.
- On redundant system ask for IPS between systems. This adds detection plus preventing adverse impact and also reduces the need for patching and extends equipment life.
- Whitelisting rather than signature-based products have longer supported product lifecycles. Place your signature-based detection on the network.
- Require aggressive and well documented hardening by the integrator. While this is only a requirement on the direct CDAs hardening reduces the need for patching.