TLP:AMBER

ELECTION INFRASTRUCTURE SUBSECTOR CYBER RISK SUMMARY

Publication: March 2021

Cybersecurity and Infrastructure Security Agency

TLP:AMBER

EXECUTIVE SUMMARY

This report provides analysis, findings, and recommendations derived from non-attributable cybersecurity trends observed between November 3, 2019, and November 3, 2020—Election Year 2020 (EY20)—among Election Infrastructure (EI) Subsector[1] entities subscribed to services provided by the Cybersecurity and Infrastructure Security Agency (CISA), specifically Cyber Hygiene (CyHy) Vulnerability Scanning and Cybersecurity Assessments services.[2] [3]

CISA's analysis of the available data for assessed EI entities found:

- 76% of EI entities for which CISA performed a Risk and Vulnerability Assessment (RVA) had spearphishing weaknesses, which provide an entry point for adversaries to launch attacks;
- 48% of entities had a critical or high severity vulnerability on at least one internet-accessible host,[4] providing potential attack vectors to adversaries;
- 39% of entities ran at least one risky service on an internet-accessible host, providing the opportunity for threat actors to attack otherwise legitimate services; and
- 34% of entities ran unsupported operating systems (OSs) on at least one internet-accessible host, which exposes entities to compromise.

CISA recommends the following mitigations to reduce EI entity risk:

- Improve phishing defenses by regularly training users, implementing email filters, deploying post-delivery protection, and conducting regular phishing assessments;
- Patch vulnerabilities on internet-accessible systems and devices on a regular schedule;
- Securely configure internet-accessible ports and services on systems and devices by implementing strong identity and access management controls, including strong passwords, multifactor authentication (MFA), and the principle of least privilege; and
- Update software and OSs to supported versions.

CISA encourages EI entities to use the findings and recommended mitigations in this report to review their cybersecurity posture and capabilities, conduct further investigations, and prioritize actions to mitigate vulnerabilities and guard against threats. Threat actors are motivated to leverage the weaknesses identified in this report to disrupt national critical functions and target EI entities that provide critical IT infrastructure to support the US elections process. CISA also encourages EI entities to email vulnerability_info@cisa.dhs.gov for additional advice and assistance.

[1] The Elections Infrastructure Subsector is within the Government Facilities Critical Infrastructure Sector. See https://www.cisa.gov/critical-infrastructure-sectors and https://www.cisa.gov/government-facilities-sector.

[2] CISA, Cyber Hygiene Services. Link: https://www.cisa.gov/cyber-hygiene-services

[3] CISA, Cyber Resource Hub, CISA Services and Assessments: https://www.cisa.gov/cyber-resource-hub

[4] Host is defined as "any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means" by the National Institute of Standards and Technology (NIST) Computer Security Resource Center. https://csrc.nist.gov/glossary/term/host.

CONTENTS

INTRODUCTION

This subsector report aggregates and analyzes EI entity data collected through CISA's CyHy vulnerability scanning service and cybersecurity assessments performed from November 3, 2019, to November 3, 2020—Election Year 2020 (EY20)—which covers the 12 months leading up to the 2020 U.S. Election Day. It provides insight into internet-accessible and internal vulnerabilities on EI entities' information technology (IT) assets to illustrate potential exposure to cyber threats. This report does *not* divulge the names of specific entities where CISA identified vulnerabilities.

Most EI is managed by state and local election entities and jurisdictions that depend on third-party providers to supply and implement the necessary IT election infrastructure and support. The fundamental IT systems required to conduct an efficient election process may include election management systems, voter registration systems and electronic poll books, ballot programmers and printers, election data solutions, and digital election supplies used to store, transport, and use equipment. This IT infrastructure has a varied attack surface and is potentially vulnerable to cyberattacks.[5]

The EI subsector is a target for:

- Advanced persistent threats (APTs) backed by foreign governments that may seek to interfere with the integrity of U.S. elections.
- Cybercriminals interested in profiting from data breaches and ransomware attacks on voter registration databases, vote tabulations, and other sensitive records and systems.[6]

In the 2016 U.S. presidential election, U.S. government reporting confirmed that Russian military actors attempted to compromise elections infrastructure within county and state elections offices and targeted the technology services provided by U.S. companies.[7] In the run-up to the 2020 election, an APT actor successfully obtained U.S. voter registration data, including in at least one instance from a state election website, and launched an election-related disinformation campaign.[8] In October 2020, CISA also observed APTs targeting elections infrastructure in state, local, tribal, and territorial (SLTT) government entities' networks. As of October 24, 2020, CISA had no evidence to indicate that integrity of elections data was compromised.[9] Well-resourced threat actors, such as APTs, may increase the potential for future elections data compromise and disruption of elections infrastructure operations.

[5] CISA, DHS Election Infrastructure Subsector-Specific Plan. 2020. https://www.cisa.gov/sites/default/files/publications/election_infrastructure_subsector_specific_plan.pdf.

[6] Center for Internet Security, EI-ISAC: Cybersecurity Spotlight – Ransomware. April 6, 2018. https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-ransomware/.

[7] Special Counsel Robert S. Mueller III, Report on the Investigation Into Russian Interference In The 2016 Presidential Election.. March 2019.. https://www.justice.gov/storage/report.pdf.

[8] CISA, Alert AA20-304A: Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data. November 3, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-304a.

[9] CISA, Alert AA20-283A: APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations. October 9, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-283a.

DATA COLLECTION METHODS AND SERVICES

Data from the following CISA services are analyzed in this report:

CyHy Automated Vulnerability Scanning tools are deployed to monitor internet-accessible systems for known vulnerabilities, configuration errors, and suboptimal security practices. CISA scans Internet Protocol (IP) addresses with the Nmap network scanner and probes responsive hosts with the Nessus vulnerability scanner to identify critical, high, medium, and low severity vulnerabilities based on the Common Vulnerability Scoring System (CVSS) version 2.0 scale of 0 to 10.[10] Nessus references the National Vulnerability Database (NVD) for its vulnerability information.[11] The NVD provides CVSS base scores and corresponding severity levels for all Common Vulnerabilities and Exposures (CVEs). Scans use the range of IP addresses provided by the scanned entity. Using these tools, CISA can identify potential and known security issues and can then recommend mitigations to the impacted stakeholder.

Cybersecurity Assessments are one-on-one engagements between CISA and an entity that combine national threat information with the vulnerabilities CISA identifies through onsite or remote assessment activities. Assessments may include internet-accessible systems and internal systems. Assessment data derives from one or more of the various CISA offerings, including scenario-based network penetration testing, web application testing, social engineering testing, wireless network testing, configuration management reviews of servers and databases, phishing assessments, and network security architecture reviews. CISA uses security-engineering experts to conduct assessments over a fixed timeframe and defines the scope of each engagement by defining IP addresses, system names, and email addresses. At the assessment's conclusion, CISA provides an entity-specific risk analysis report that includes actionable remediation recommendations prioritized by risk. From November 3, 2019, to November 3, 2020, EI entities participated in the following assessments:

- **Risk and Vulnerability Assessments (RVAs)** collect data through assessments and combine it with national threat and vulnerability information, in order to provide an organization with actionable remediation recommendations prioritized by risk. This assessment is designed to identify vulnerabilities that adversaries could exploit to compromise network security controls.
- **Remote Penetration Tests (RPTs)** simulate the tactics and techniques used by real-world adversaries to identify and validate exploitable pathways. This service is designed for testing perimeter defenses, the security of externally available applications, and the potential for exploitation of open-source information.
- **Phishing Campaign Assessments (PCAs)** evaluate an organization's susceptibility and reaction to phishing emails of varying complexity.

While the entities analyzed in this report do not represent a rigorous statistical depiction of all the complex and varied EI entities in the United States, CISA encourages all EI entities to adopt the recommendations and best practices, as applicable.

[10] Forum of Incident Response and Security Teams (FIRST), Common Vulnerability Scoring System (CVSS). https://www.first.org/cvss/.

[11] National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD). https://nvd.nist.gov/.

EI ENTITY STATISTICS

301 EI entities were scanned by the CyHy Vulnerability Scanning service by the end of EY20. Over the course of EY20, EI entities scanned in CyHy increased from 233 to 301, and hosts scanned increased from 53,034 to 66,011.

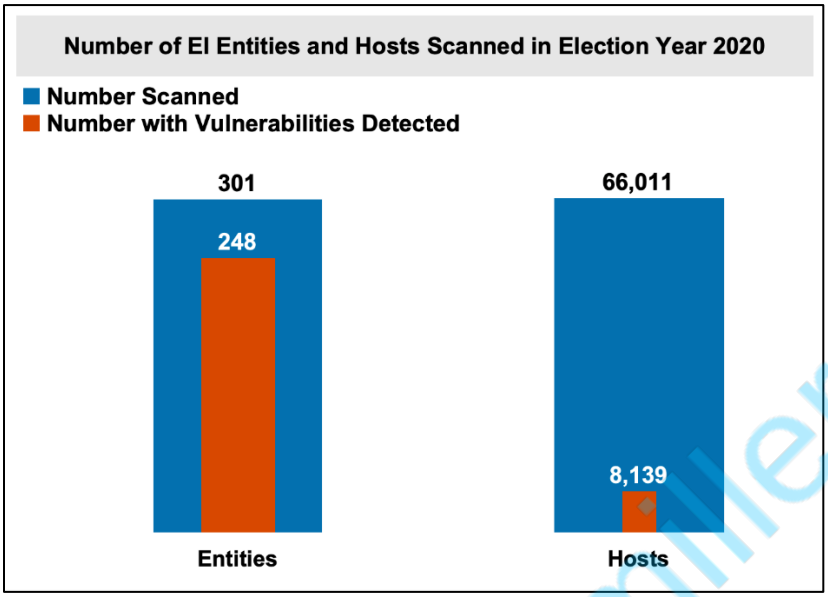

Figure 1: EI CyHy Stakeholders in EY20

As the tool scans additional hosts—due to continual enrollment of EI entities——CISA anticipates it will detect a growing number of hosts with vulnerabilities. Trending analyses presented in this report provide metrics that control for and normalize the impact of continual enrollment.

CISA performed 124 assessments for EI entities in EY20 (see figure 2). Assessment findings identified specific gaps in the cybersecurity posture of individual organizations. When aggregated, these findings present common attack paths and weaknesses that attackers may use to breach entities' defenses and bypass implemented controls. EI entities can learn from these findings to improve their defenses.

CISA Assessments of EI Entities by Type

PCA	RPT	RVA	Total
16	97	11	124

Figure 2: CISA Assessments of EI Entities by Type in EY20

VULNERABILITY SCANNING FINDINGS AND ANALYSIS

Vulnerability Trends of EI Entities

During EY20, CyHy scanning detected 48,796 total vulnerabilities on hosts in the 324 participating EI entities. Of those vulnerabilities, 319 (0.80 percent) were critical severity and 1,820 (4.55 percent) were high severity based on CVSS base score (see figure 3).

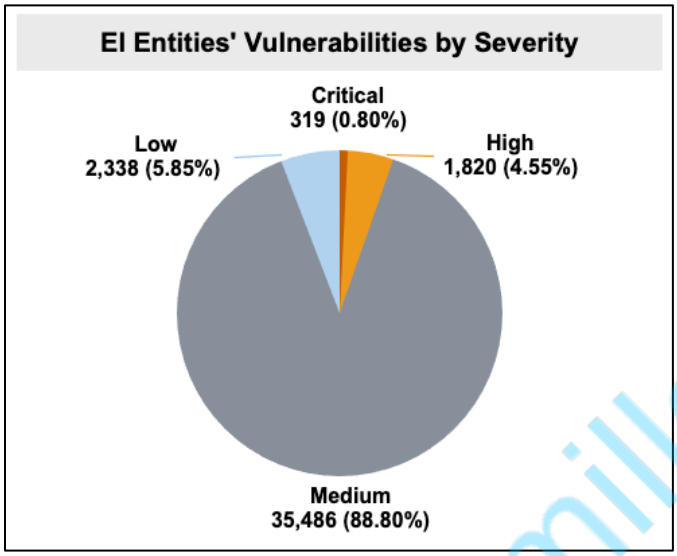

Figure 3: EI EY20 Vulnerabilities by Severity

Vulnerability Remediation

Median Days to Remediate

Identifying vulnerabilities allows CISA to notify the affected entities and evaluate entities' remediation efforts. CISA considers a vulnerability remediated when CyHy scanning no longer identifies it on the host. CISA, and enrolled entities, can measure the effectiveness of vulnerability management by examining the number of days between initial detection and remediation. The median number of days to remediate provides an indication of how long it takes entities to reduce their exposure to vulnerabilities.

During EY20, the median days to remediate vulnerabilities for EI entities was 103.7 days for critical severity vulnerabilities, and 91.9 days for high severity vulnerabilities (see figure 4). Vulnerabilities that remain open for extended periods could allow malicious actors to compromise election-related networks through exploitable, externally facing systems. As a best practice, and as required for federal civilian entities pursuant to federal directives, CISA recommends that critical and high severity vulnerabilities on internet-accessible hosts be remediated within 15 and 30 days, respectively.[12] Entities are also encouraged to manage vulnerabilities by adopting a risk-based approach.[13]

[12] DHS, Binding Operational Directive 19-02. April 29, 2019. https://cyber.dhs.gov/bod/19-02/.

[13] NIST Cybersecurity Framework. April 2018. https://www.nist.gov/cyberframework/framework.

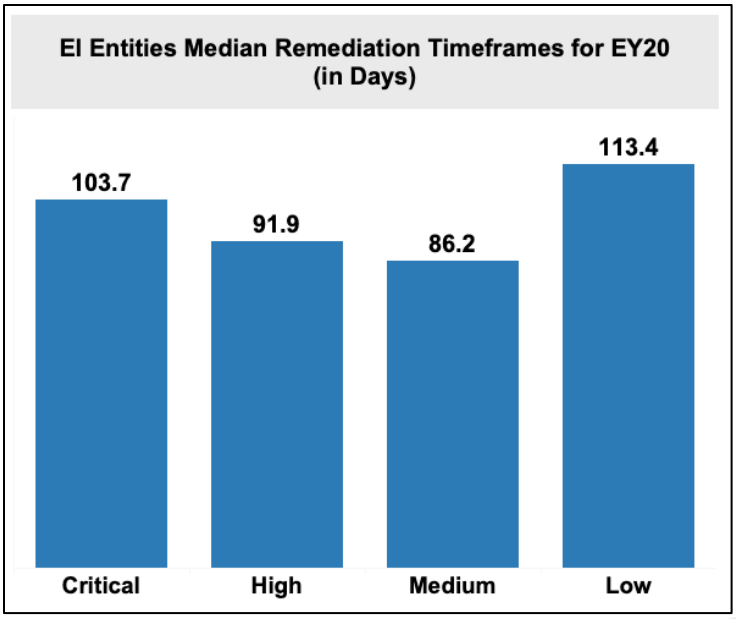

Figure 4: EY20 Median Remediation Timeframes

Medium and low severity vulnerabilities also have the potential to impact EI entities, as their presence on a network perimeter could act as a launch point or become part of a chain of vulnerabilities used to perpetuate an attack. CISA has observed APTs exploiting multiple legacy vulnerabilities in combination with newer privilege escalation vulnerabilities to facilitate attacks. This commonly used tactic, known as *vulnerability chaining*, exploits multiple vulnerabilities during a single intrusion to compromise a network or application.[14]

Once the median time to remediate is evaluated, organizations should dive deeper into remediation performance by analyzing vulnerability based on additional metrics. CISA analyzed and identified trends in EI entities' remediation prioritization by grouping vulnerabilities based on remediation timeframes (see figure 5).

Total Vulnerabilities Remediated by Severity

Severity	<30 Days Old	30-90 Days Old	90+ Days Old	Severity Total
Critical	72	45	125	242
High	247	207	480	934
Medium	5,050	6,296	7,025	18,371
Low	289	202	657	1,148
Grand Total	5,658	6,750	8,287	20,695

Figure 5: EI Vulnerability Remediation Timeframes

[14] CISA, Alert AA20-283A: APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations. October 24, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-283a.

During EY20, 125 critical and 480 high severity vulnerabilities were remediated in over 90 days. The longer a vulnerability remains active on an internet-accessible host, the more time a threat actor has to identify the weakness and launch an attack. The identified vulnerabilities were eventually remediated; however, for over 90 days, they presented a known weak point in the network perimeter that adversaries could target and attempt to exploit.

Vulnerabilities with Known Exploits

CISA encourages entities to remediate internet-accessible vulnerabilities as quickly as possible; however, due to resource constraints and entity priorities, not every vulnerability can be remediated quickly. The threat actor decision to spend time and resources weaponizing a vulnerability is dependent on multiple vulnerability traits. Cybersecurity researchers contend that only 2 to 5 percent of published vulnerabilities are ever weaponized by threat actors for use in an attack—i.e., exploit code or malware is only developed for a small subset of vulnerabilities.[15]

Targeting remediation efforts on vulnerabilities with known exploits can help entities prioritize the vulnerabilities most likely to be targeted by threat actors. For example, remediation of a newly discovered, highly prevalent, and publicly exploited vulnerability on an entity's high-value system should warrant a higher priority. Prioritization, based on contextual factors, aligns with the Stakeholder-Specific Vulnerability Categorization (SSVC) model, which considers exploitation as one of the factors entities should consider in the management and prioritization of active vulnerabilities.[16]

In EY20, CISA's vulnerability scanning of EI entities identified vulnerabilities with known exploits across all severity categories. For example, during EY20's first quarter (Q1), CISA identified 6.8 percent of scanned EI entities had critical severity vulnerabilities with known exploits on at least one host (see Figure 6); and per Figure 4, critical severity vulnerabilities with known exploits were remediated in 108 median days. CISA recommends that entities prioritize remediating vulnerabilities with the highest severity and likelihood for exploitation first. A wide array of adversaries (sophisticated and unsophisticated) target vulnerabilities that have known exploits. Such targets require relatively fewer resources to exploit and provide attackers a higher probability of success in gaining access to an entity's network.

[15] Jay Jacobs, Sasha Romanosky, Benjamin Edwards, Michael Roytman, Idris Adjerid. "Exploit Prediction Scoring System (EPSS)," Blackhat 2019, August 13, 2019. https://arxiv.org/abs/1908.04856.

[16] Carnegie Mellon University Software Engineering Institute, Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization, December 2019. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=636379.

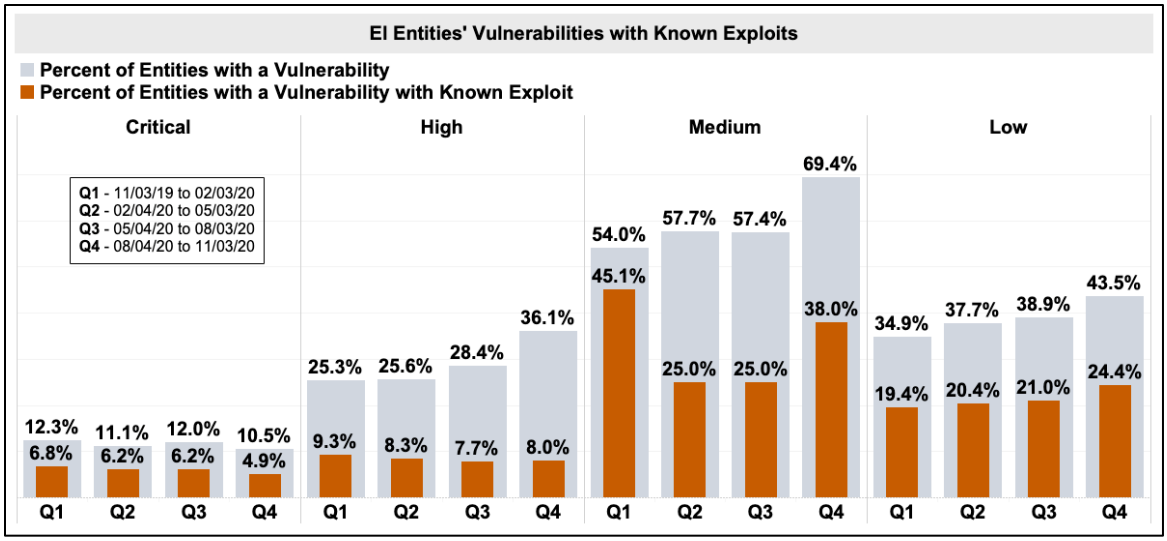

Figure 6: EI Entity Vulnerabilities with Known Exploits

Vulnerability Backlog

Unpatched vulnerabilities that persist on internet-accessible hosts for a prolonged timeframe present an opportunity for attackers. Measures of vulnerability management should consider both the vulnerabilities remediated and those that remain unpatched during a particular timeframe. Vulnerability backlog is the quantity of active vulnerabilities over a timeframe. This measure provides insight into entities' vulnerability management processes and how well they can address influxes of new vulnerabilities while simultaneously reducing the backlog of existing vulnerabilities. Remediation of more vulnerabilities than those that are opened during a given timeframe provides a positive indication that an entity is keeping pace with or reducing their vulnerability backlog.

During EY20, the average backlog of vulnerabilities per EI entity peaked at 86.2 vulnerabilities per entity in Q2, then improved over the course of the year with a final average of 74.2 vulnerabilities per entity in Q4 (see figure 7). Newly opened vulnerabilities per entity drove the backlog changes, which include only vulnerabilities first identified in a quarter and still active at the end of that quarter.

By the end of EY20, there was a slight increase in the average number of existing vulnerabilities per entity. This finding may indicate that network defenders face challenges in clearing existing vulnerabilities out of their backlogs as they identify new ones. If this trend persists or increases, it can present an opportunity for threat actors to take advantage of older vulnerabilities that remain unremediated.

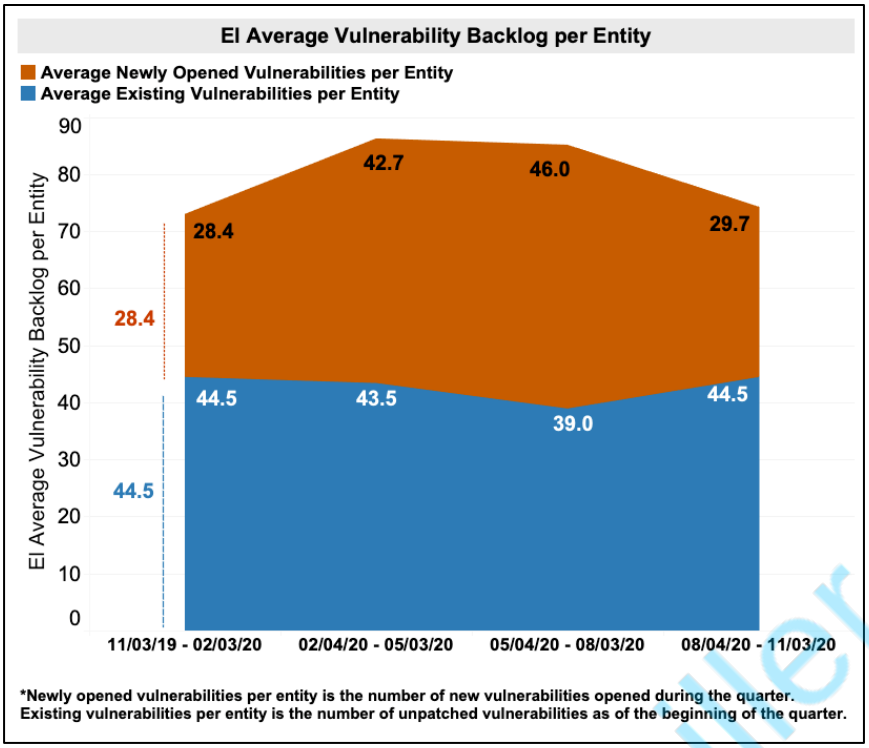

Figure 7: Average Vulnerability Backlog Over Time

Prevalent Vulnerabilities

CISA analyzed the data to identify specific vulnerabilities that were prevalent across EI entities in EY20. The top five most prevalent critical severity vulnerabilities appeared in multiple entities and hosts across the Subsector and exposed common issues facing the Subsector (see figure 8).

The most prevalent high severity vulnerability among the scanned EI entities was SSL Version 2 and 3 Protocol Detection (see figure 8).[17] CISA recommends that all EI entities examine their ingress traffic for deprecated versions of SSL and work to remediate or mitigate this vulnerability.

[17] The SSL Version 2 and 3 Protocol Detection vulnerability occurs when a remote service accepts encrypted connections using SSL version 2 or 3, both of which are impacted by several cryptographic flaws that can be used by threat actors to compromise the confidentiality and integrity of network communications.

Top Five Most Prevalent Critical Vulnerabilities			
Vulnerability	**CVE**	**Entities Impacted**	**Hosts Impacted**
PHP Unsupported Version Detection		22	37
Microsoft Windows Server 2003 Unsupported Installation Detection		14	25
Unix Operating System Unsupported Version Detection		14	24
Microsoft IIS 6.0 Unsupported Version Detection		14	22
OpenSSL Unsupported		9	10

Top Five Most Prevalent High Vulnerabilities			
Vulnerability	**CVE**	**Entities Impacted**	**Hosts Impacted**
SSL Version 2 and 3 Protocol Detection		112	778
Unsupported Web Server Detection		78	300
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability	CVE-2019-11043	19	64
SSH Protocol Version 1 Session Key Retrieval	CVE-2001-1473	18	33
Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	CVE-2017-7679	11	24

Figure 8: Top 5 Most Prevalent Critical and High Vulnerabilities Detected by CyHy in EY20

Many of the top five most prevalent critical and high severity vulnerabilities discovered were due to hosts using unsupported software, protocols, and OS versions.[18] Unsupported products provide threat actors an incentive to attack as they can easily target known weaknesses in these products to compromise target networks and systems.

Entities and Hosts Running Unsupported OS Versions

Beyond identifying specific vulnerabilities in products, CISA's scanning tools can typically identify the OS version running on remotely accessible hosts, which allows CISA to determine if an entity has a weakness due to an unsupported OS version. By the end of EY20, CISA had identified unsupported OS versions for 1.1 percent of scanned EI hosts and 33.6 percent of scanned EI entities (see figure 9).[19]

[18] Unsupported software, protocols, and OS versions usually mean that no new security patches for the product will be released by the vendor and, as a result, the product likely contains security vulnerabilities.

[19] The scanning tools identified OS for approximately 92 percent of hosts scanned during the year. In addition, only unsupported versions of Windows 7, Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008 are considered unsupported OS by the scanning tools. Hosts with unknown OS are factored into the overall hosts for the percentage calculation of unsupported OS versions.

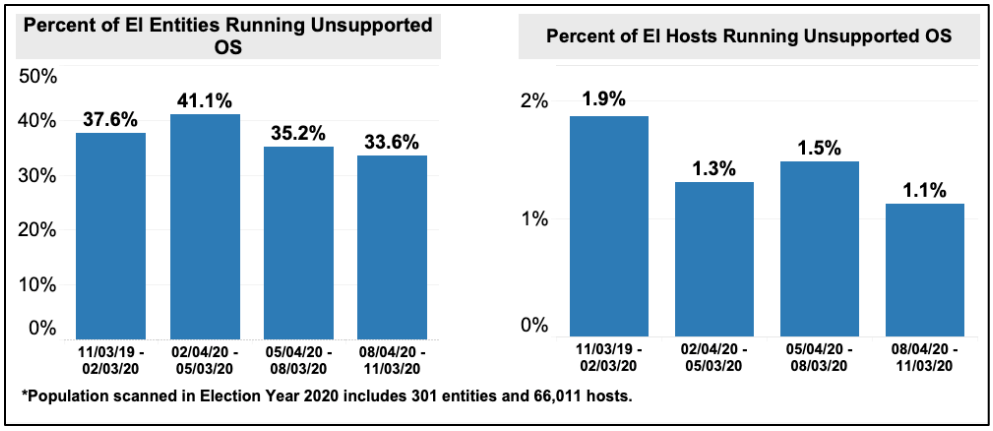

Figure 9: Percent of EI Entities and Hosts Running Unsupported OS Versions

Throughout EY20, the percent of hosts running unsupported OS versions decreased, which is a positive indicator of EI entities limiting their exposure and vulnerability by removing or upgrading OS versions. By the end of EY20, only 1.11 percent of scanned hosts were running unsupported OS versions. Although the percent of entities running unsupported OS versions also decreased, there were still 33.6 percent of entities running at least one instance of unsupported OSs. CISA encourages EI entities to continue this progress by phasing out all unsupported OS versions and staying informed of vendor and manufacturer end-of-support notifications.

Potentially Risky Services

In addition to vulnerabilities and unsupported OS versions, hosts are running potentially risky services with known weaknesses and vulnerabilities. When exposed to the internet and unsecured, these are additional entry points for threat actors to launch and orchestrate remote attacks on networks.

Based on available research and threat information, CISA scans for 10 potentially risky services that can increase an entity's risk of exposure (see Appendix A). CISA identified that 39 percent of scanned EI entities and 2 percent of scanned EI entities' hosts were operating potentially risky services exposed to the internet (see figure 10).

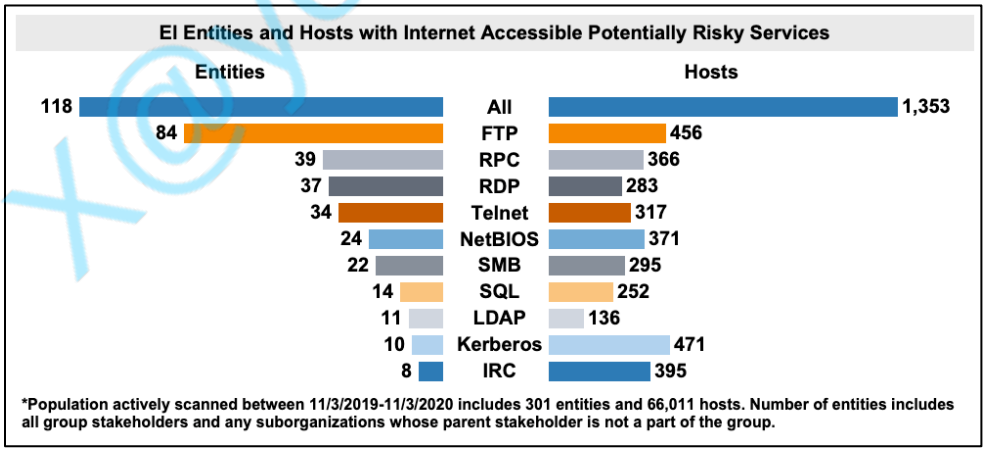

Figure 20: EI Entities and Hosts Running Risky Services on Open Ports

Of the 10 risky services examined, File Transfer Protocol (FTP) was the most prevalent, identified for 28 percent of entities, and Remote Procedure Call (RPC) was identified in 13 percent of entities (see figure 11). FTP facilitates the transfer of files sent on a network over plain text, or unencrypted protocol; and RPC can be leveraged by malicious actors to facilitate privilege escalation attacks.[20] An FTP service operated without secure encryption exposes entities to threat actors who can steal sensitive data. For example, CISA observed threat actors employing LokiBot malware to steal passwords and credentials from entities that use FTP.[21]

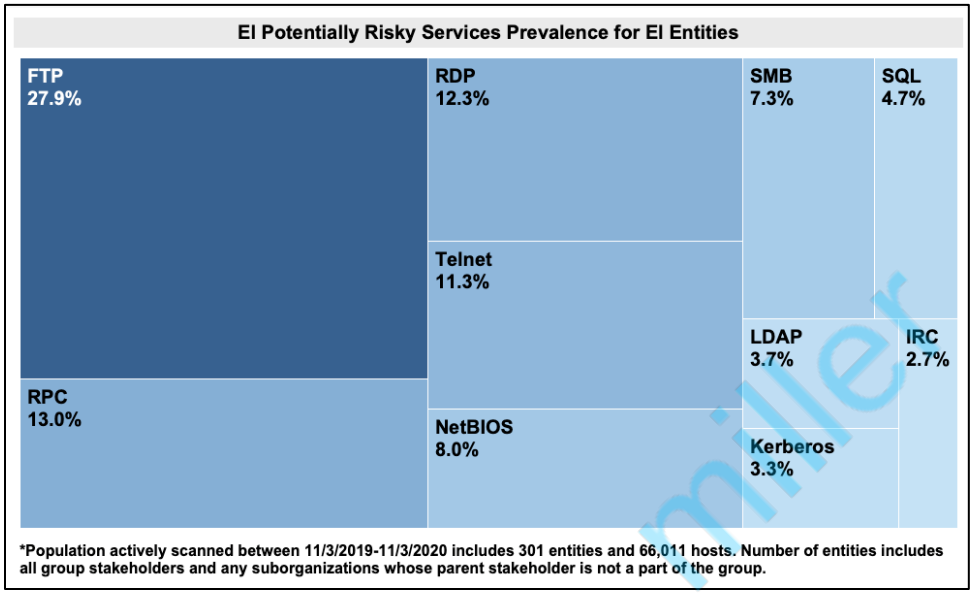

Figure 31: EI Entities Running Risky Services on Open Ports

Similarly, CISA observed threat actors leveraging Remote Desktop Protocol (RDP), which allows remote connection to a computer over a network, to launch attacks against entities from multiple sectors, including SLTT entities.[22,23] Although not as common, 12.3 percent of EI entities had at least one internet-accessible host running RDP. Due to the commonality of attacks involving RDP, entities that have not secured it are susceptible to exploitation by threat actors who are actively targeting RDP as part of their attack path.

[20] CISA, Alert AA20-283A: APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations. October 24, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-283a.

[21] CISA, Alert AA20-266A: LokiBot Malware. October 24, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-266a.

[22] CISA, Alert AA20-283A: APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations. October 24, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-283a.

[23] CISA, Alert AA20-014A: Critical Vulnerabilities in Microsoft Windows Operating Systems. January 14, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-014a.

CISA ASSESSMENT FINDINGS

Aggregated analysis of findings from CISA assessments highlights commonalities across assessed EI entities. The presented findings should be evaluated by all EI entities but should not be viewed as systemic problems across the EI subsector. [24]

RVA and RPT Findings

In EY20, CISA performed RPTs and RVAs for 108 EI entities. RPT and RVA teams performed penetration tests, phishing assessments, web application assessments, and database assessments. These teams identified 451 findings (see figure 12), which are vulnerabilities and weaknesses that present a risk to the entity. Although not a statistically significant sample that can be generalized to the Subsector, EI entities should be aware of these findings.

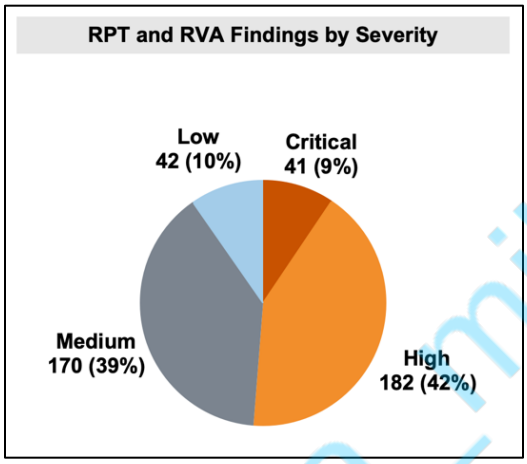

Figure 12: RPT and RVA Findings by Severity

CISA's findings are categorized by a severity schema described in detail in Appendix B. The 9 percent of findings that were critical severity are vulnerabilities that pose an immediate and severe risk to the entity's IT environment due to the ease of exploit and potential impact. The 42 percent of findings that were high severity include weaknesses or vulnerabilities that an adversary may be able to use to exercise full control on a target device if the vulnerability were to be exploited.

During the assessments, spearphishing weaknesses were the most common finding observed in 73 percent of entities (see figure 13). The broad success of spearphishing indicates that assessed entities possessed inadequate border and host-level protections. This weakness allowed spearphishing emails to pass through the network border and subsequently execute on the local host with the aid of a user performing some action, like clicking a link or opening a file that initiates the execution of malicious payloads. In addition to indicating a lack—or poor implementation—of technological protections, this finding can also indicate a lack of cybersecurity awareness and recognition of spearphishing by users, which leaves the entity vulnerable. This finding is

[24] The entities analyzed in this report do not represent a rigorous statistical depiction of all the complex and varied EI entities in the United States.

significant for all EI entities to review and address, as many threat actors regularly initiate attacks by employing spearphishing to capture credentials and establish initial remote access.

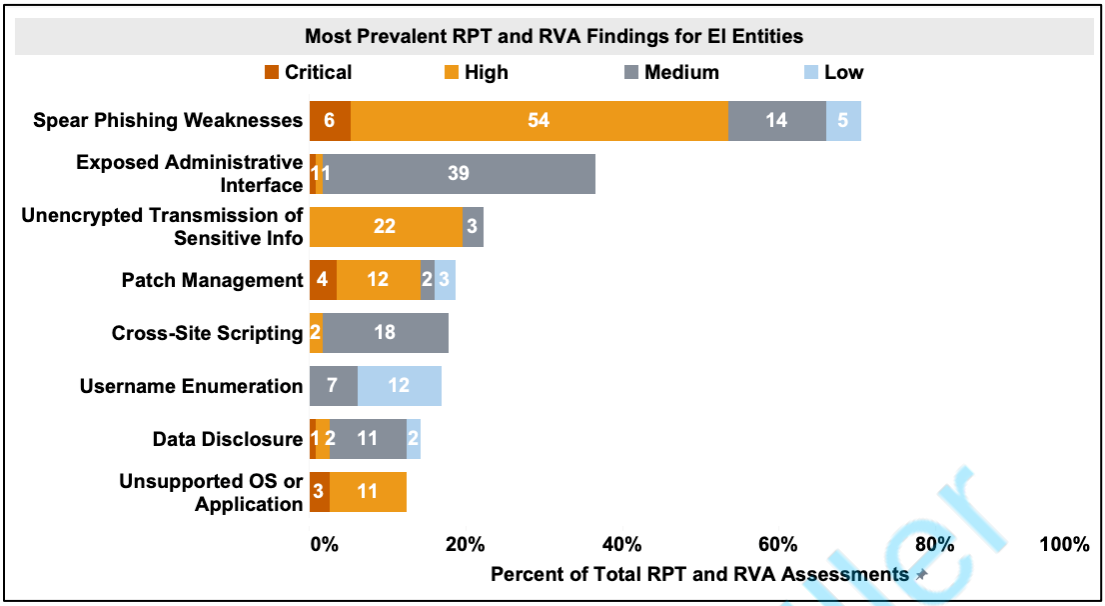

Figure 13: Most Prevalent Findings from RVA and RPT Assessments in EI Entities for EY20

The next most frequent findings were exposed administrative interfaces, unencrypted transmission of sensitive data, and patch management.

- Exposed administrative interfaces may increase likelihood of unauthorized access to entity management and administrative functions;
- Unencrypted transmission creates an easy target for attackers to capture sensitive data; and
- Failing to apply the latest patches can leave a system open to attack via publicly available exploits.

EI entities could make it more difficult for adversaries to attack by reducing the exposure of administration interfaces, encrypting transmission of sensitive information, and patching systems.

RVA Attack Paths

Threat actors use combinations of successful tactics, techniques, and procedures (TTPs)—also known as the attack path —to deliver malicious payloads and cause disruption on victim systems and networks. During RVA penetration testing, CISA assessment teams mimic adversary TTPs to simulate attack scenarios from initial access to exfiltration to inform entities of gaps in their defenses. CISA uses the MITRE Enterprise Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework to categorize the success of attempted TTPs (see Figure 14).[25]

[25] CISA analyzed and mapped all FY19 RVA findings to the MITRE ATT&CK framework to provide critical infrastructure entities with lists of observed successful attack paths: https://www.cisa.gov/publication/rva-mapped-mitre-attck-framework-infographic.

Most Effective MITRE ATT&CK Tactics and Techniques from RVAs		
Tactics	**Techniques**	**% Success**
1. Initial Access	Spearphishing Link	72.7%
2. Execution	PowerShell	81.8%
3. Persistence	Valid Accounts	9.1%
4. Privilege Escalation	Access Token Manipulation	18.2%
	Process Injection	18.2%
	Valid Accounts	18.2%
5. Defense Evasion	Mshta	27.3%
	Obfuscated Files or Information	27.3%
6. Credential Access	Credential Dumping	90.9%
7. Discovery	Account Discovery	81.8%
8. Lateral Movement	Pass the Hash	81.8%
9. Collection	Data from Local System	54.5%
10. Command and Control	Commonly Used Port	90.9%
11. Exfiltration	Exfiltration Over Command and Control Channel	45.5%

Figure 44: Most Frequently Effective RVA Tactics and Techniques for EI Entities

Figure 14 identifies the most frequently effective TTPs observed in RVAs. While this is not an exhaustive list of all MITRE ATT&CK TTPs,[26] they are tactics and techniques commonly used by adversaries to orchestrate attacks. Techniques that were most frequently effective in these RVAs are described in further detail to help network defenders understand the potential actions adversaries might take to exploit EI entity networks.

- *Spearphishing Links* [T1566.002] were used regularly to provide initial access points. Using links to download malware contained in email, instead of attaching malicious files to the email itself, avoids defenses that may inspect email attachments.
- *PowerShell* [T1059.001] was used to download and execute malicious payloads.
- *OS Credential Dumping* [T1003], *Account Discovery* [T1087], and *Pass the Hash* [T1550.002] techniques were used in coordination to obtain credentials, enumerate accounts, and move laterally through a network. These techniques allowed adversaries to bypass access controls and move between systems to reach their targets.
- Commonly Used Ports (*Application Layer Protocol* [T1071]) were used to disguise malicious network traffic during communications with command and control servers.
- Common themes noted across these techniques include nefarious use of tools in Windows platforms and masking malicious intentions under the guise of legitimate operations.

PCA Findings

Phishing remains a primary technique for gaining initial access to target organizations. CISA conducts PCAs to observe the percentage of users who click on test phishing emails relative to the total population of users who receive a phishing email (termed the user click rate). The PCA process focuses on measuring user behavior and therefore relies on an entity allowing CISA phishing emails to bypass filters and defenses that could prevent the email from reaching a user. PCA results can indicate the success—or failure—of user awareness and training regarding phishing and other forms of social engineering.

[26] MITRE ATT&CK, Enterprise Tactics. January 27, 2021. https://attack.mitre.org/tactics/enterprise/.

EI entities had a click rate of 17.4 percent in EY20 (see figure 15). That was 7.8 percent higher than the 9.6 percent click rate for all other SLTT and Critical Infrastructure (CI) entities during EY20 (figure 16). A single click on a phishing email can begin an attack chain leading to network compromise. Entities should implement efforts—such as training users and promoting awareness—to minimize this attack vector.

Election Year 2020 Phishing Campaign Assessment Findings for EI Entities								
Total Assessments	Total Campaigns	Emails Sent	Unique Clicks	Click Rate	User Reports	Report Rate	Average Time to First Click	Average Time to First Report
16	108	16,329	2,840	17.4%	1,498	9.2%	6:15 Minutes	5:53 Minutes

Figure 55: PCA Statistics for EI Entities in EY20

Election Year 2020 Phishing Campaign Assessment Findings for SLTT and CI (Excluding EI Entities)								
Total Assessments	Total Campaigns	Emails Sent	Unique Clicks	Click Rate	User Reports	Report Rate	Average Time to First Click	Average Time to First Report
26	150	53,986	5,206	9.6%	3,715	6.9%	3:55 Minutes	3:28 Minutes

Figure 66: PCA Statistics for all other SLTT and CI in EY20

An important counter-phishing method is training users how to manage suspicious emails, including where to send the email for inspection. Once a phishing email campaign has been reported, entity security teams can take steps to mitigate the attack. The report rate is a metric CISA uses to measure entities' ability to defend against phishing; it tallies the number of user reports of phishing emails (i.e., when a user notifies their organization's IT security of the suspicious email). While EI entities had a higher click rate than all other SLTT and CI entities, they also had a higher report rate of 9.2 percent compared to the 6.9 percent report rate for all PCAs CISA conducted in EY20.

OBSERVATIONS, MITIGATIONS, AND BEST PRACTICES

The following recommendations and mitigations are based on the analysis and findings of the CISA vulnerability scanning and assessments outlined above. CISA provides these recommendations to help EI entities reduce exposure to vulnerabilities and defend against threats. However, these recommendations do not guarantee protection against all cybersecurity risks impacting the EI Subsector. CISA encourages EI entities to use these recommendations to review their cybersecurity posture and capabilities, conduct further investigation, and prioritize actions to mitigate vulnerabilities and guard against threats.

Phishing Susceptibility

Observation: Successful phishing attacks allow an attacker initial access to an entity's network. RPT and RVA teams were able to bypass email filtering controls to launch spearphishing attacks in 73 percent of EI assessments. In addition, EI entity personnel were found to be susceptible to phishing attacks in PCAs; PCAs for EI entities had a 17.4 percent click rate compared to a 9.2 percent report rate for phishing emails.

Mitigation: Entities can reduce their workforce's phishing susceptibility through increased user awareness training and simulations. Additionally, entities can block most common phishing attacks by implementing automated border and host-level protections. EI entities should regularly analyze these protections—including spam-filtering capabilities—to ensure their continued effectiveness in blocking the delivery and execution of malware.

Best Practice: Train users, operators, and security personnel on how to prevent and reduce social engineering susceptibility, report incidents, and initiate incident response procedures.[27,28] Develop and test incident response plans and procedures.

Patch Management

Observation: Threat actors scan for and target vulnerable internet-accessible hosts to launch attacks. CISA scanning indicated that 48 percent of EI entities experienced a critical or high severity vulnerability on at least one internet-accessible host during EY20. The median days to remediate vulnerabilities for EI entities was 103.7 days for critical severity vulnerabilities and 91.9 days for high severity vulnerabilities. In addition, the average backlog of vulnerabilities per EI entity peaked at 86.2 vulnerabilities per entity, then improved over the course of the year with a final average of 74.2. Entities with a large vulnerability backlog over time have a higher likelihood that one or more of those vulnerabilities will be used as part of an attack.

Mitigation: CISA recommends regularly scanning internet-accessible hosts and remediating critical and high severity vulnerabilities within 15 and 30 days, respectively. Entities should modify patch management strategies to prioritize patching critical severity vulnerabilities with proven exploits on high-impact systems first, and reduce time to remediate vulnerabilities. Additionally,

[27] CISA, Capacity Enhancement Guide: Counter-Phishing Recommendations for Non-Federal Organizations. October 8, 2020. https://www.cisa.gov/sites/default/files/publications/Capacity_Enhancement_Guide-Counter-Phishing-Recommendations_for_Non-Federal_Organizations.pdf.

[28] CISA, CISA Insights: Enhance Email and Web Security. September 25, 2019. https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-EnhanceEmailandWebSecurity_S508C-a.pdf.

entities should continue to reduce the backlog of vulnerabilities, especially those with known exploits that could be used to breach the defensive perimeter.

Best Practice: Prioritize remediation of vulnerabilities using a risk-based approach that considers likelihood of attack, ease of exploitation, and the magnitude of potential impact. Consider remediating active vulnerabilities with known exploits first, and defining vulnerability prioritization mechanisms that consider contextual factors specific to each entity, such as the SSVC framework.[29] Follow established enterprise network best practices for IT infrastructure, including the implementation of a strong patching methodology for OSs, applications, and firmware.[30]

Unsupported Operating System Versions

Observation: Threat actors target unsupported OS versions because their lack of security patches and updates increases the ease of exploitation. In the three months leading up to the 2020 Election Day, 34 percent of observed EI entities had at least one internet-accessible host running an unsupported OS version.

Mitigation: Entities should identify and plan upgrades for aging systems, and replace end-of-support components when possible with supported and secure versions. When replacement is not possible, organizations should use network segmentation for vulnerable systems.

Best Practice: Entities should consider leveraging strategic and long-term measures to identify and replace IT—including software, firmware, OSs, and hardware—that is no longer supported. Entities should ensure exceptions are isolated if replacement is not a viable option.

Potentially Risky Services

Observation: Potentially vulnerable, risky services like FTP, RPC, and RDP, that are exposed to the internet present possible entry and escalation points for attackers. Throughout EY20, 39 percent of EI entities scanned were running at least one potentially risky service on an internet-accessible host.

Mitigation: Entities should restrict, secure, and patch potentially risky services exposed to the internet and assess their legitimate business use cases. In some cases, operating potentially risky services with a level of security control is acceptable, such as connecting through virtual private networks (VPNs), using multifactor authentication (MFA), and using secure encryption.[31] [32]

Best Practice: Securely configure or completely limit internet-accessible assets to only those needed to run entity operations. Isolate high-value assets, including operational technology systems, from the internet whenever possible. Use network segmentation to create layers of defense to protect critical systems and assets.

---

[29] Carnegie Mellon University Software Engineering Institute, Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization, December 2019. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=636379.

[30] CISA, Security Tip ST19-002: Best Practices for Securing Election Systems. May 21, 2019, Updated: November 02, 2020. https://us-cert.cisa.gov/ncas/tips/ST19-002.

[31] CISA, Alert AA20-073A: Enterprise VPN Security. April 15, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-073a.

[32] NSA, Cybersecurity Information sheet::Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations. January 5, 2021. https://us-cert.cisa.gov/ncas/current-activity/2021/01/05/nsa-releases-guidance-eliminating-obsolete-tls-protocol.

CONCLUSION

EI entities can significantly reduce their cybersecurity risk by performing additional investigation and analysis of the findings described in this report. CISA encourages entities to implement standard cyber hygiene practices and applicable mitigations identified in this report to reduce their exposure. EI entities are welcome to seek additional advice and assistance from CISA via vulnerability_info@cisa.dhs.gov and adopt additional best practices found in the Center for Internet Security (CIS) Handbook for Elections Infrastructure Security.[33]

Feedback regarding this product is critical to CISA's continuous improvement. If you have feedback specific to your experience with this product, please send CISA your input by filling out the CISA Product Survey.

[33] Center for Internet Security (CIS), Handbook for Elections Infrastructure Security. Link: https://www.cisecurity.org/elections-resources/elections-infrastructure-handbook-best-practices/

APPENDIX A: POTENTIALLY RISKY SERVICES

Table 1: Most Common Potentially Risky Services Identified for Scanned EI Entities

Service	Description
FTP	File Transfer Protocol (FTP) is used for the transfer of files between a client and server on a network over a clear-text, or unencrypted, protocol. Cleartext passwords used for authentication are susceptible to sniffing, spoofing, and brute force attacks that can lead to data loss and unauthorized internal network access.
IRC	Internet Relay Chat (IRC) is an unencrypted protocol that facilitates communication in the form of text for group communication. Threat actors may be able to gather sensitive information from IRC communications between users, and launch denial of service attacks on IRC traffic to disrupt user to user interaction.
Kerberos	Kerberos is a computer-network authentication protocol that facilitates communication over a non-secure network in a more secure manner. Unpatched Kerberos connections may allow a threat actor to authenticate onto an entity's network to conduct malicious activity under a legitimate guise.
LDAP	Lightweight Directory Access Protocol (LDAP) is an application protocol that allows clients to perform a variety of operations in a directory server. When exposed to the internet, LDAP could be used by threat actors to gather and manipulate sensitive information related to users, systems, services, and applications on a network.
NetBIOS	Network Basic Input/Output System (NetBIOS) is an unauthenticated protocol that allows applications on computers to communicate over a local area network. When NetBIOS is exposed to the internet, attackers may be able to reach directories, files, and gather sensitive information from devices communicating over the network.
RDP	Remote Desktop Protocol (RDP) allows remote connection to a computer over a network, which can be exploited when misconfigured. RDP should be kept internal to an organization's network and multifactor authentication (MFA) should be used to secure access. Threat actors can use RDP to facilitate data theft and exposure, hijacking login credentials, malware, and ransomware.
RPC	Remote Procedure Call (RPC) enables data exchange and functionality from a different location on the computer, network, or across the internet. Leaving RPC open to the internet may enable threat actors to penetrate the defensive perimeter, exfiltrate data, and modify configurations.
SMB	Server Message Blocks (SMB) is a protocol that provides shared access to files, printers, and serial ports between nodes on a network. SMB lacks support for secure authentication protocols.

SQL	Standard Query Language (SQL) is a standard computer language for managing data held in a relational database, and used to query, insert, update, and modify data. Insecure implementations of SQL can be leveraged by threat actors to retrieve sensitive data over database interfaces.
Telnet	Teletype Network (Telnet) is an application protocol used on the internet or local area network for unencrypted text communications. It poses a severe security risk when exposed to the internet, as attackers can see and manipulate the traffic to and from devices with ease.

APPENDIX B: RVA AND RPT SEVERITY RATING CRITERIA

Table 2: Severity Rating Criteria

Severity	Description
Critical	Critical vulnerabilities pose an immediate and severe risk to the environment because of the ease of exploit and potential severe impact. Critical items are reported to the customer immediately.
High	Intruders may be able to exercise full control on the targeted device. Following are examples: • Easily exploitable vulnerabilities that can lead to complete application, system, or network compromise, such as an intruder having the ability to remotely administer files on a web server • Severe router/firewall/server misconfigurations • Worm, Trojan, or backdoor detection • Vulnerability that has tools readily available on the Internet to exploit • Weak passwords for remote administration and users
Medium	Intruders may be able to exercise some control of the targeted device. Following are examples: • Disclosure of unauthorized sensitive customer information or user account information • Ability of an intruder to obtain full read access to corporate confidential information • Lack of basic logging and alerting capabilities • Antivirus misconfigurations • Untrusted networks having access to trusted networks
Low	The vulnerabilities discovered are reported as items of interest but are not normally exploitable. Many low-severity items reported by security tools are not included in this report because they are often informational, unverified, or of minor risk.
Informational	These vulnerabilities are potential weaknesses within the system that cannot be readily exploited. These findings represent areas of which the customer team should be cognizant, but they do not require any immediate action.

APPENDIX C: COMMON RVA FINDINGS

Table 3: Common RVA Findings for Scanned EI Entities

Finding Name	Finding	Standard Remediation
Spearphishing Weakness	Successful spearphishing requires an attacker's email to pass through the network border and execute on the local host with the aid of a user performing some action. Most common phishing attacks can be rebuffed by good border and host-level automated protections. Inadequate protections allow the execution of malicious payloads.	Regularly analyze border and host-level protections, including spam-filtering capabilities, to ensure their continued effectiveness in blocking the delivery and execution of malware.
Exposed Administrative Interface	An exposed administrative interface can enable an unauthorized user to access management and administrative functions of the device or application. This type of access is typically restricted and usually does not include additional layers of access control. An attacker can conduct a brute force attack against an administrative interface that places no restrictions on login attempts.	Properly restrict access to management and configuration interfaces and other potentially sensitive files on remotely accessible web servers, applications, and services. Use multi-factor authentication for all administrative access.
Unencrypted Transmission of Sensitive Info	Unencrypted transmission of data allows an attacker to intercept traffic between two systems or endpoints and recover any information traversing the channels in cleartext. Usernames and passwords are some of the types of data that can be obtained by passing unencrypted data across the network.	Configure systems and applications to use encrypted communications mechanisms that comply with applicable federal standards, industry best practices, and/or agency-defined requirements.
Patch Management	Patches and updates are released to address existing and emerging security threats and address multiple levels of criticality. Failure to apply the latest patches can leave the system open to attack with publicly available exploits.	Enforce consistent patch management across all systems and hosts within the network environment. Where patching is not possible due to limitations, implement network segmentation to limit exposure of the vulnerable system or host. Deploy automated patch management tools on all systems for which such tools are available and safe.

Finding Name	Finding	Standard Remediation
Cross Site Scripting	Cross-Site Scripting (XSS) attacks are a type of injection attack. An attacker can inject unsanitized malicious scripts into a parameter to later be executed by an unsuspecting user. These malicious scripts can access the user's cookies, the user's current session (through session cookies), or other sensitive data used to access the site. Once the malicious script is stored on the server, any other user visiting the site or application could view and execute it.	Implement server-side controls to whitelist the character sets that are allowed as input into web application fields. The applications should reject anything outside of that approved input. In addition, review the application's system development lifecycle (SDLC) to determine how to incorporate input validation.
Username Enumeration	Username enumeration allows an attacker to identify valid usernames within an organization. The valid usernames can then be used to gain unauthorized access to an application, service, or system as a valid user.	Restrict service access and implement generic error messages for incorrect username attempts. Institute maximum login attempts rules to limit the availability of this attack vector.
Data Disclosure	Sensitive data disclosure occurs when information that should be guarded is available publicly or to unprivileged or lower-privileged users. This information may include business data, application information, system information, or other environmental data that should not be shared due to security concerns.	Implement a secure configuration for devices and applications containing sensitive data. Ensure that publicly accessible data--including operational items such as error/warning messages--does not reveal information that can be used by an attacker. Verify that system configurations and applications meet security standards. Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.

Finding Name	Finding	Standard Remediation
Unsupported OS or Application	Using software or hardware that is no longer supported by the vendor poses a significant security risk because new and existing vulnerabilities are no longer patched. There is no way to address security vulnerabilities on these devices to ensure that they are secure. This puts the overall security posture of the entire network at risk because an attacker can target these devices to establish an initial foothold into the network.	Evaluate the use of unsupported hardware and software and discontinue where possible. If discontinuing the use of unsupported hardware and software is not possible, implement additional network protections to mitigate the risk.