TLP:AMBER

HEALTHCARE AND PUBLIC HEALTH SECTOR CYBER RISK SUMMARY

Publication: April 2021

Cybersecurity and Infrastructure Security Agency

TLP:AMBER

EXECUTIVE SUMMARY

This report provides findings, analysis, and recommendations derived from non-attributable cybersecurity vulnerability trends observed between October 2018 and September 2020 among Healthcare and Public Health (HPH) Sector entities that subscribed to services provided by the Cybersecurity and Infrastructure Security Agency (CISA). The sample analyzed includes 192 HPH entities enrolled in Cyber Hygiene (CyHy) Vulnerability Scanning during FY20 and 33 Cybersecurity Assessments performed by CISA for HPH entities during FY19 and FY20.[1]

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

- 96% of Risk and Vulnerability Assessments (RVAs) reported social engineering weaknesses, which provide entry points for adversaries to launch attacks;
- 69% of participating entities experienced a critical or high vulnerability on at least one internet accessible host, providing attack vectors to adversaries;
- 54% of participating entities ran unsupported operating systems (OSs) on at least one internet-accessible host at the end of 2020, which exposes entities to compromise; and
- 49% of participating entities ran at least one risky service on an internet-facing host, providing opportunities for threat actors to attack otherwise legitimate services.

CISA recommends the following mitigations to reduce HPH entity risk:

- Patch vulnerabilities on internet-accessible systems and devices on a regular schedule;
- Improve phishing defenses by regularly training users, implementing email filters, deploying post-delivery protection, and conducting regular phishing simulations;
- Update software and OS to supported versions; and
- Securely configure internet-accessible ports and services on systems and devices.

CISA encourages HPH 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 attack HPH entities to disrupt national critical functions. CISA also encourages HPH entities to email vulnerability_info@cisa.dhs.gov for additional advice and assistance and to sign up for CyHy Vulnerability scanning and Cybersecurity Assessments.

[1] Due to the COVID-19 pandemic, several FY20 assessments were cancelled. FY19 assessment data was included to supplement FY20 data.

CONTENTS

INTRODUCTION

This sector report aggregates and analyzes Healthcare and Public Health (HPH) entity data collected through CISA's CyHy vulnerability scanning service throughout U.S. Federal Government Fiscal Year (FY) 2020 and cybersecurity assessments performed during FY19 and FY20.[2] It provides insight into vulnerabilities on HPH 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.

Threat actors may actively leverage the weaknesses identified in this report to target HPH entities and potentially disrupt national critical functions. CISA encourages HPH entities to review the findings and recommended mitigations in this report to evaluate their cybersecurity posture and capabilities, conduct further investigations, and prioritize actions to mitigate vulnerabilities and guard against threats.

The HPH Sector is large and diverse, and includes both the public and private sector entities. It includes hospitals, healthcare facilities, research centers, suppliers, manufacturers, and IT providers. The Sector requires interconnected IT systems to securely access, store, and transmit large amounts of HPH data—such as protected health information, research, and intellectual property—to optimize healthcare services and outcomes.

The HPH Sector is a target for:

- Advanced persistent threats (APTs) seeking to obtain economic advantage, and
- Cybercriminals interested in profiting from data breaches and ransomware payments.

For much of FY20, threat actors sought to take advantage of the COVID-19 pandemic, placing additional strain on HPH entities. APTs backed by foreign governments targeted entities involved in vaccine research and development, storage, and transportation to collect intelligence and gain a competitive advantage.[3,4,5]

Meanwhile, financially motivated threat actors targeted the critical IT systems of other HPH entities–such as hospitals–with ransomware.[6] As HPH entities become more dependent on internet-connected medical devices, cloud storage services, and networked systems, threat actors

---

[2] For reference, U.S. government fiscal year (FY) 2020 was October 1, 2019 to September 30, 2020. This report analyzes the results of CISA's CyHy Vulnerability Scanning of 192 HPH entities enrolled in FY20 and 33 assessments performed by CISA for HPH entities in FY19 and FY20. Due to the COVID-19 pandemic, several FY20 assessments were cancelled; therefore, FY19 assessment data was included to supplement the lack of FY20 data.

[3] HHS, APT and Cybercriminal Targeting of HCS. June 9, 2020, https://www.hhs.gov/sites/default/files/apt-and-cybercriminal-targeting-of-hcs.pdf.

[4] FBI, Press Release, People's Republic of China (PRC) Targeting of COVID-19 Research Organizations. May 13, 2020. https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations.

[5] CISA, Current Activity, IBM Releases Report on Cyber Actors Targeting the COVID-19 Vaccine Supply Chain, December 03, 2020. https://us-cert.cisa.gov/ncas/current-activity/2020/12/03/ibm-releases-report-cyber-actors-targeting-covid-19-vaccine-supply.

[6] CISA, Alert AA20-302A: Ransomware Activity Targeting the Healthcare and Public Health Sector. November 2, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

will likely continue targeting them. HPH entities that highly rely upon health IT are particularly vulnerable due to uptime requirements for systems that support patient health outcomes.

DATA COLLECTION METHODS AND SERVICES

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

CyHy Automated Vulnerability Scanning tools are frequently 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) scale of 0 to 10. Nessus references the National Vulnerability Database (NVD) for its vulnerability information. The NVD provides CVSS 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 a sector 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. Assessments may include internet-accessible systems and internal systems. At the assessment's conclusion, CISA provides an entity-specific risk analysis report that includes actionable remediation recommendations prioritized by risk. In FY19 and FY20, HPH entities participated in the following assessments:

- **Risk and Vulnerability Assessments (RVAs)** collect data through onsite 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 HPH entities in the United States, CISA encourages all HPH entities to adopt the recommendations and best practices, as applicable.

HPH ENTITY STATISTICS

CISA evaluated 192 entities enrolled in the CyHy Vulnerability Scanning service during FY20. The number of HPH entities enrolled in vulnerability scanning increased from 112 to 192 (see figure 1). The 71 percent increase in HPH entity enrollment showcases CISA's ongoing efforts to support the HPH Sector during the challenges of the COVID-19 pandemic.

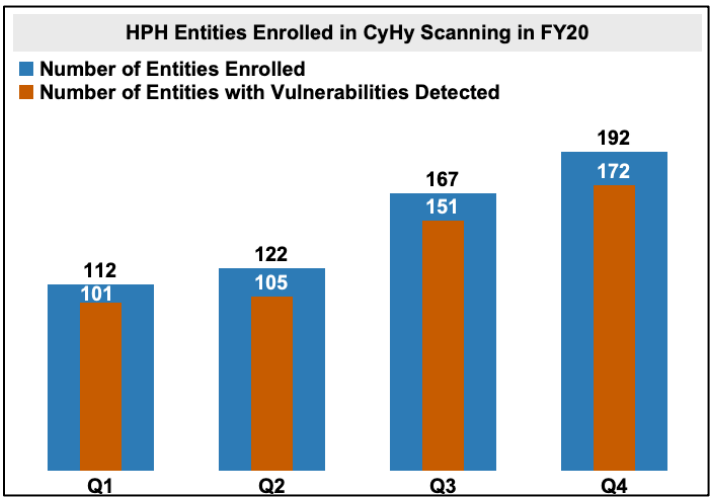

Figure 1: HPH CyHy Stakeholders in FY20

Trending analyses presented in this report provide metrics that control for and normalize the impact of continual enrollment. As the number of enrolled entities increased throughout FY20, there was not an overall rise in the percent of entities with vulnerabilities detected, which remained between 86 and 90 percent. Continued enrollment of HPH entities also increased the total number of hosts scanned and, as a result, identified an increase of the number of hosts with vulnerabilities detected. During FY20, vulnerabilities were detected for 30 to 39 percent of the total hosts scanned (see figure 2). Despite an increase in the total number of entities and hosts scanned, there was not a significant change in the percentage of hosts with vulnerabilities detected.

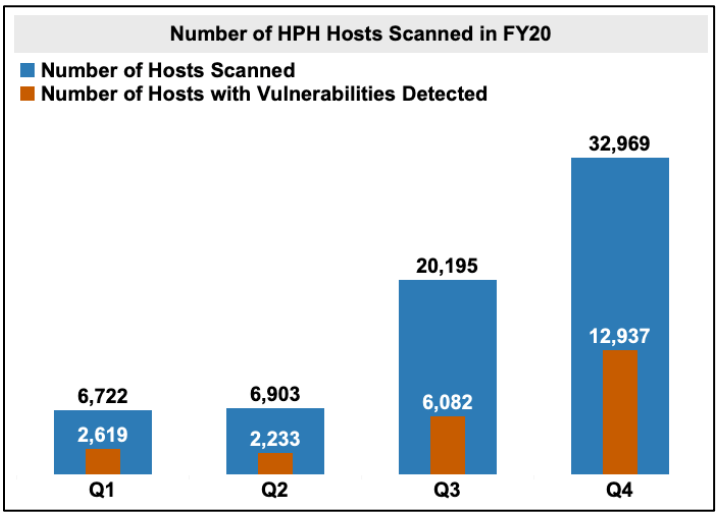

Figure 2: Number of HPH Hosts Scanned in FY20

This report analyzes 33 assessments performed by CISA for HPH entities in FY19 and FY20 (see figure 3). Assessment findings identify specific gaps in the cybersecurity posture of individual organizations. When aggregated, these findings present common attack paths and weaknesses that attackers use to breach entities' defenses and bypass implemented controls. HPH entities can learn from the common attack paths and weaknesses to improve their defenses.

CISA Assessments by Type

	PCA	RPT	RVA	FY Total
FY19	1		1	2
FY20	4	20	7	31
Grand Total	5	20	8	33

Figure 3: CISA Assessments by Type

VULNERABILITY SCANNING FINDINGS AND ANALYSIS

Vulnerability Trends of HPH Sector Entities

When CISA's CyHy vulnerability scanning identifies critical and high vulnerabilities it sends impacted entities notification within 24 hours of detection. This allows entities to patch and secure their perimeter defenses against threat actors who may actively target known vulnerabilities. During FY20, the 192 HPH entities participating in the CyHy vulnerability scanning program experienced a total of 64,128 vulnerabilities. Of those vulnerabilities, 464 (0.72 percent) were critical and 2,695 (4.20 percent) were high severity based on CVSS impact score (see figure 4).

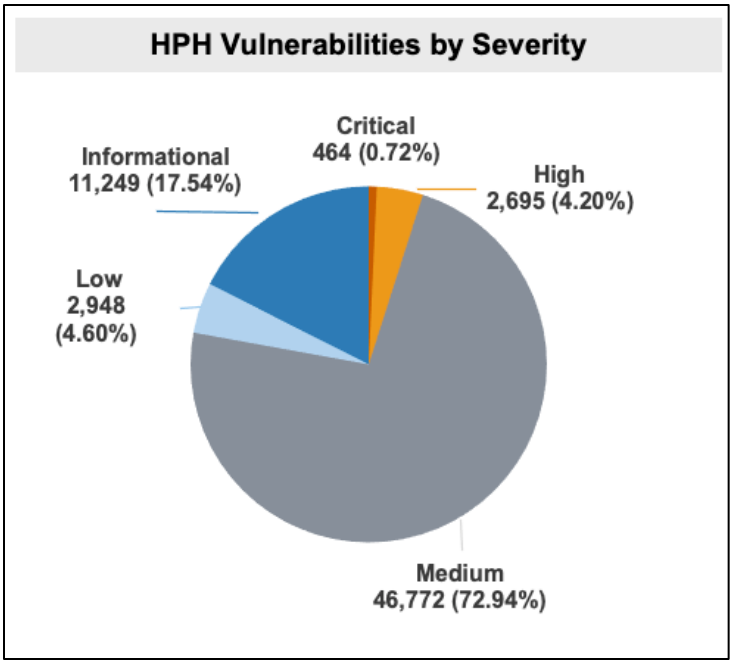

Figure 4: HPH Vulnerabilities by Severity

Vulnerability Remediation

Median Days to Remediate

Identifying vulnerabilities allows CISA to evaluate entities' remediation efforts. CISA considers a vulnerability remediated when CyHy scanning no longer identifies it on the host. CISA, and 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 FY20, the median days to remediate vulnerabilities for HPH entities was 24.9 days for critical vulnerabilities and 57.6 days for high vulnerabilities (see figure 5). The median days to remediate these vulnerabilities for HPH entities presents a concern for potential exploitation. As a best practice, and in accordance with federal directives, CISA recommends that critical and high vulnerabilities on internet-accessible hosts be remediated within 15 and 30 days, respectively. HPH entities remediation rates lagged behind the remediation rate of federal agencies, but were comparative to other critical infrastructure sectors.

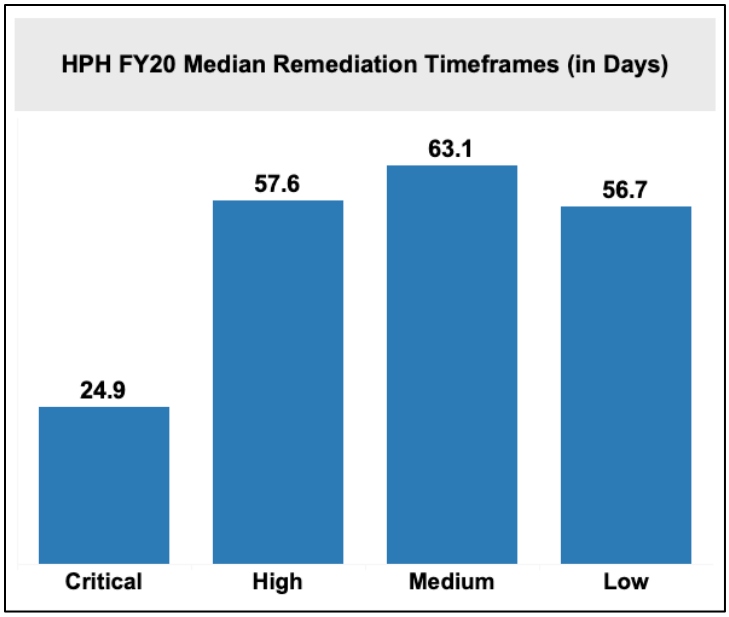

Figure 5: HPH FY20 Remediation Timeframes

In most cases, CISA encourages prioritizing remediation of critical vulnerabilities first, then high, medium and low. Critical and high severity vulnerabilities typically provide the most potential access to a network for a threat actor. If resources are limited, CISA recommends patching critical and high vulnerabilities with known exploits first, then the remainder of critical and high vulnerabilities, and then medium and low vulnerabilities with known exploits. Entities that are effectively prioritizing patch management based on vulnerability severity should have the lowest median days to remediate for critical vulnerabilities, followed by high, medium, then low.

Based on median time to remediate, HPH entities remediated critical vulnerabilities faster than all other severity types in FY20. However, for the 1,289 high vulnerabilities that HPH entities patched in FY20, the median number of days to remediate was 57.6 days, which is over twice the number of days to remediate for critical vulnerabilities—a concerning finding.

Medium and low severity vulnerabilities also have the potential to impact HPH 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.[7]

Median days to remediate does not tell the entire story of all vulnerabilities remediated for HPH entities during the year. CISA analyzed and identified trends in the HPH entities' remediation prioritization by grouping vulnerabilities based on remediation timeframes (figure 6).

[7] CISA, Alert AA20-283A: APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations. November 2, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-283a.

Total Vulnerabilities Remediated by Severity				
Severity	**<30 Days Old**	**30-90 Days Old**	**90+ Days Old**	**Severity Total**
Critical	182	39	58	279
High	654	248	387	1,289
Medium	9,160	6,113	3,792	19,065
Low	708	346	270	1,324
Grand Total	10,704	6,746	4,507	21,957

Figure 6: Remediated Vulnerabilities

During FY20, 58 critical and 387 high vulnerabilities were not remediated for over 90 days. This is concerning because the longer a vulnerability remains unpatched 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-facing vulnerabilities as quickly as possible; however, due to resource constraints and entity priorities, not every vulnerability can be remediated immediately. Many risk tolerance calculations factor in that only 2 to 5 percent of published vulnerabilities are ever weaponized by threat actors—i.e., exploit code or malware is only developed for a small subset of vulnerabilities.[8]

In FY20, CISA's vulnerability scanning of HPH entities identified vulnerabilities with known exploits across all severity categories. During FY20's third quarter (Q3), 9.6 percent of HPH entities identified critical vulnerabilities with known exploits; similarly, during Q2, 13.9 percent of HPH entities identified high vulnerabilities with known exploits (figure 7). 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 critical and high vulnerabilities that have known exploits. Such targets require fewer resources to exploit and provide attackers a higher probability of success in gaining access to an entity's network.

[8] 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.

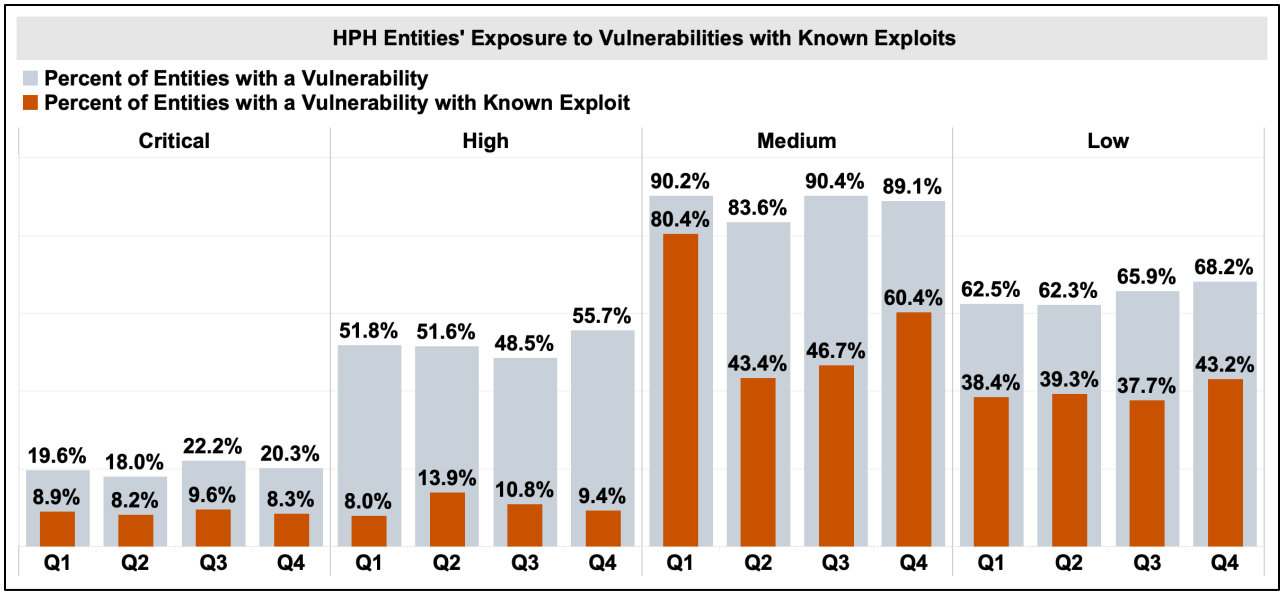

Figure 7: HPH Stakeholder Vulnerabilities with Known Exploits

Critical vulnerabilities with known exploits impacted between 8.2 and 9.6 percent of scanned HPH entities on a quarter to quarter basis during FY20. Most of these were remote code execution vulnerabilities, which allow a remote attacker to take control of devices on a network.

Vulnerability Backlog

Unpatched vulnerabilities that persist on internet-facing hosts for a prolonged timeframe present opportunity for attackers. Measures of vulnerability management should consider both the vulnerabilities remediated and those that remain active during a 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 are able address influxes of new vulnerabilities while simultaneously reducing a 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.

HPH entities began FY20 Q1 with an average of 77 vulnerabilities per entity but this average increased rapidly over the course of the year with a final average of 260.7 vulnerabilities per entity (figure 8). There are multiple contributing factors to the increase in vulnerability backlog, including:

- A large number of HPH entities joined CyHy in Q3 and Q4; these new entities account for 67 percent of the total vulnerabilities for the year. One entity, added in Q4, contributed 11,550 (18 percent) of the year's total vulnerabilities.
- Four prevalent vulnerabilities drove the counts higher during the second half of the year:
    1. Potentially Risky Service Detected: Microsoft Remote Procedure Call (MSRPC),
    2. Transport Layer Security (TLS) Version 1.0 Protocol Detection,
    3. HTTP Strict Transport Security (HSTS) Missing from HTTPS Server, and
    4. TLS Version 1.1 Protocol Detection.

The overall increase in average number of vulnerabilities among HPH entities may indicate that network defenders face challenges in clearing 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 unpatched.

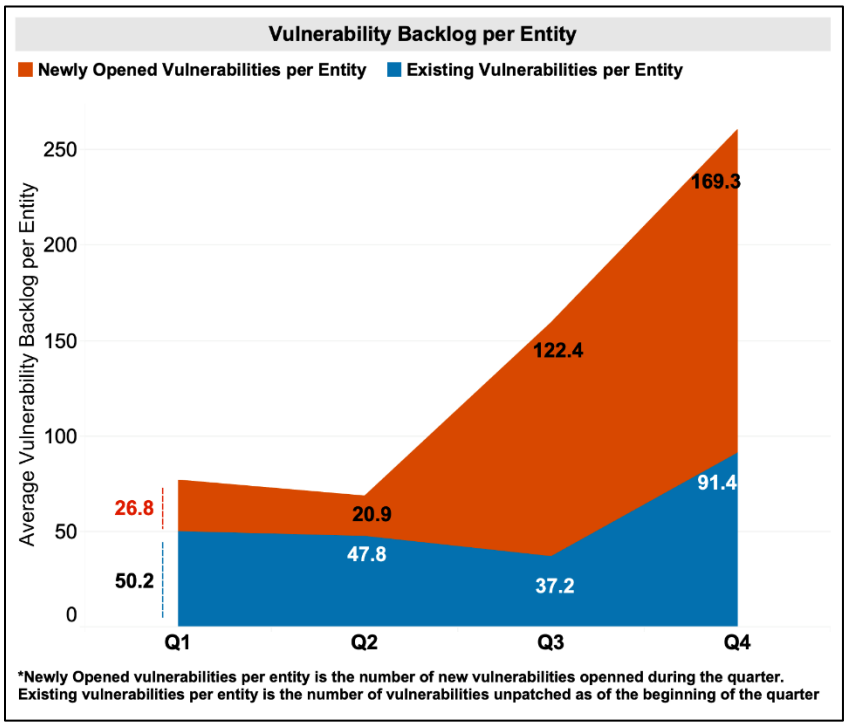

Figure 8: Vulnerability Backlog per Entity

Prevalent Vulnerabilities

CISA analyzed the data to identify specific vulnerabilities that were prevalent across HPH entities in FY20 (figure 9). Of the 464 critical vulnerabilities identified, the Hypertext Preprocessor (PHP) Unsupported Version Detection vulnerability was the most prevalent critical vulnerability, impacting 23 entities and 92 hosts.[9]

The most prevalent high severity vulnerability impacting the scanned HPH entities was Secure Socket Layer (SSL) Version 2 and 3 Protocol Detection (figure 9).[10] Because of its prevalence (found on 111 entities' systems), CISA recommends that all HPH entities examine their scanning data and ensure that they can remediate or mitigate it.

[9] Unsupported version detection means the vendor is no longer providing security patches for the product and, as a result, the software running on the host likely contains vulnerabilities that could be exploited by a threat actor.

[10] 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 confidentiality in network communications and mask malicious activity during data transfer.

Top Five Overall Critical Vulnerabilities			
Vulnerability	**CVE**	**Entities Impacted**	**Hosts Impacted**
PHP Unsupported Version Detection		23	92
Microsoft IIS 6.0 Unsupported Version Detection		16	54
Microsoft Windows Server 2003 Unsupported Installation Detection		16	40
Unix Operating System Unsupported Version Detection		11	21
Microsoft Exchange Server Unsupported Version Detection (Uncredentialed)		11	18
Top Five Overall High Vulnerabilities			
Vulnerability	**CVE**	**Entities Impacted**	**Hosts Impacted**
SSL Version 2 and 3 Protocol Detection		111	1,195
Unsupported Web Server Detection		83	566
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.	CVE-2019-11043	22	72
Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	CVE-2017-7679	18	28
SSH Protocol Version 1 Session Key Retrieval	CVE-2001-1473	11	44

Figure 9: Top 5 Critical and High Vulnerabilities detected by CyHy in FY20

Many of the top five prevalent critical and high vulnerabilities discovered were due to hosts using unsupported software, protocols, and OS versions.[11] 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.

Hosts Running Unsupported OS Versions

Beyond identifying specific vulnerabilities in products, CISA's scanning tools can identify the OS version running on hosts, which allows CISA to determine if an entity has a weakness due to an unsupported OS version. By the end of FY20, CISA had identified unsupported OS versions for 3,221 (10 percent) of the 34,950 HPH scanned hosts (figure 10).[12]

[11] 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.

[12] The scanning tools were able to identify OS for approximately 73% of hosts scanned during the year. In addition, the scanning tools define unsupported versions of Windows 7, Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008 as unsupported OS.

HPH Entities and Hosts Running Unsupported OS				
	Q1	Q2	Q3	Q4
Entities with at Least One Host Running End of Support OS	69 (63%)	64 (54%)	83 (51%)	102 (54%)
Hosts Running End of Support OS	501 (7%)	388 (6%)	526 (3%)	3,221 (10%)
Population Scanned in FY20:		188 Entities	34,950 Hosts	

Figure 10: HPH Entities and Hosts Running Unsupported OS

Throughout FY20, the number of hosts running unsupported OS versions increased, which is a concerning indicator of an expanding attack surface for HPH entities. CISA encourages HPH entities to reduce this risk by phasing out all unsupported OS versions and staying informed of vendor end-of-support notifications. Planning for either system upgrades or system decommissioning can help reduce potential exposure to vulnerabilities in unsupported systems.

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 49 percent of scanned HPH entities (93 out of 188) and 9 percent of scanned hosts (3,030 out of 34,950) during FY20 were operating potentially risky services exposed to the internet (figure 11).

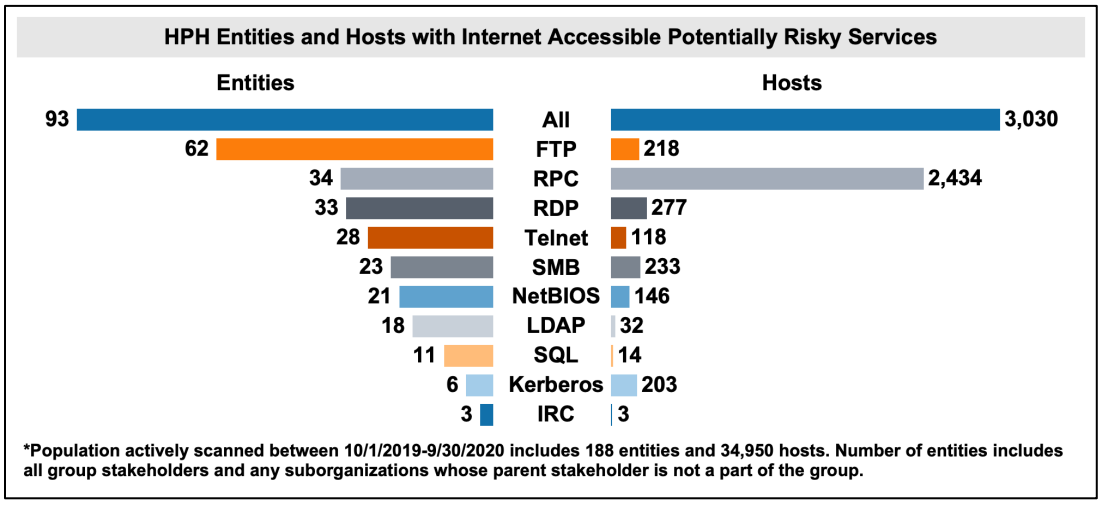

Figure 11: HPH Entities and Hosts Running Risky Services on Open Ports

Of the 10 risky services examined, File Transfer Protocol (FTP) was the most prevalent, identified for 33 percent of entities (figure 12). FTP facilitates the transfer of files sent on a network over plain text, or unencrypted, protocol. 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.[13]

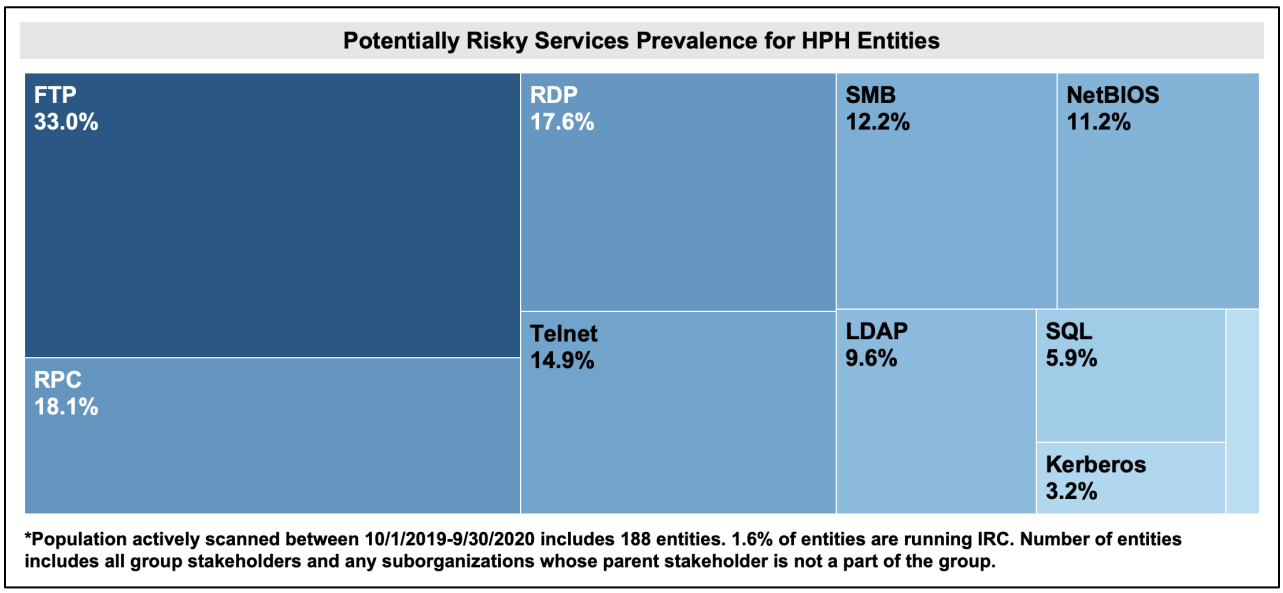

Figure 12: HPH Entities Running Risky Services on Open Ports

Similarly, CISA observed threat actors leveraging Remote Desktop Protocol (RDP), which allows remote connection to a computer over a network, to launch attacks against public and private HPH Sector entities.[14,15,16] Although not as common, 17.6 percent of entities had at least one internet-facing host running RDP. Due to the commonality of attacks involving RDP—specifically in the HPH Sector—entities that have not secured it are susceptible to exploitation by threat actors who are actively targeting RDP as part of their attack path.

Vulnerabilities Grouped by CPE Details

CISA analyzed the prevalence of vulnerabilities by vendor to gain insight into the supply chain of specific open-source and third-party dependencies that may be vulnerable to exploit by threat actors. To evaluate vulnerabilities by vendor, CISA leveraged the Common Platform Enumeration

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

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

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

[16] CISA, Alert AA20-302A: Ransomware Activity Targeting the Healthcare and Public Health Sector. November 2, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

(CPE) tagging for the products impacted by identified vulnerabilities.[17] It should be noted that only 16 percent (10,569 out of 64,128) of vulnerabilities identified by CISA during FY20 were associated with a vendor based on CPE (figure 13). The other 53,550 vulnerabilities did not have an associated CPE.

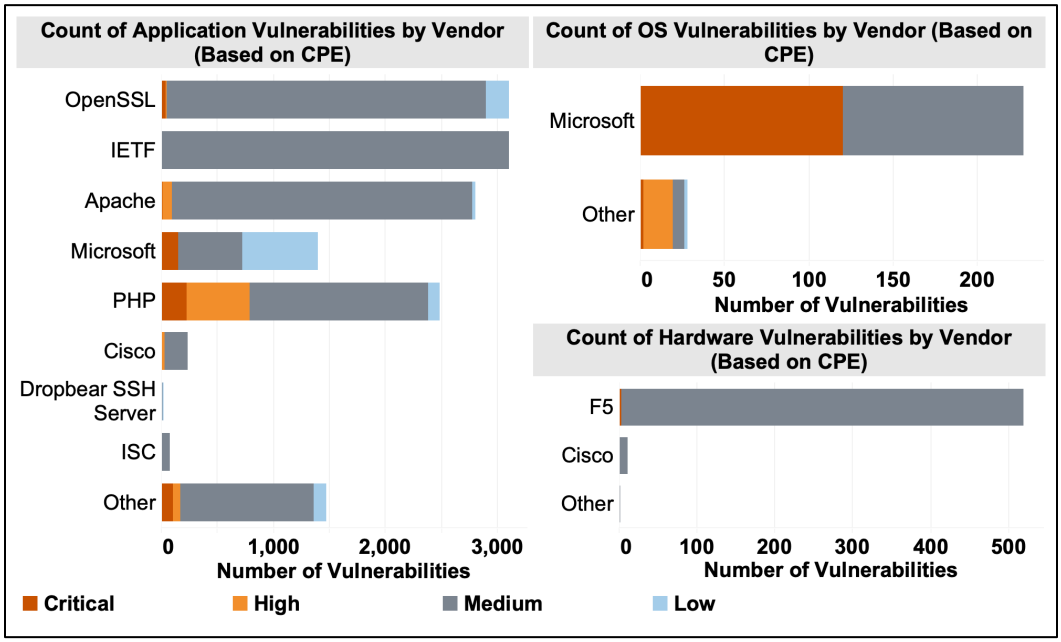

Figure 13: Vulnerability Count by Vendor in FY 2020

OpenSSL and the Internet Engineering Task Force (IETF) applications had the most vulnerabilities. These organizations provide software tools—including cryptographic protocols—designed to encrypt communications over a computer network but can introduce vulnerabilities when older, deprecated versions of the protocols are used. CISA encourages HPH organizations to be aware of the vulnerabilities in open-source products like OpenSSL and their prevalence in the software supply chain, which can be exploited by attackers.

CISA ASSESSMENT FINDINGS

Aggregated analysis of findings from CISA assessments highlight commonalities across assessed HPH entities. The presented findings should be evaluated by all HPH entities, but should not be viewed as systemic problems in the HPH Sector (due to the limited number of Sector entities assessed).

RVA and RPT Findings

In FY19 and FY20, CISA performed RVAs and RPTs for 25 HPH entities. RVA and RPT teams performed penetration tests, phishing assessments, web application assessments, and database

[17] CPE is a standardized method of describing and identifying classes of information technology systems, software, and packages. The National Institute of Standards and Technology (NIST) hosts and maintains the official CPE dictionary: https://nvd.nist.gov/products/cpe#:~:text=CPE%20is%20a%20structured%20naming%20scheme%20for%20information,for%20binding%20text%20and%20tests%20to%20a%20name.

assessments. These teams identified 202 findings (figure 14), which are vulnerabilities and weaknesses that present a risk to the entity. Although not a statistically significant sample that can be generalized to the sector, HPH entities should be aware of occurrence of these findings.

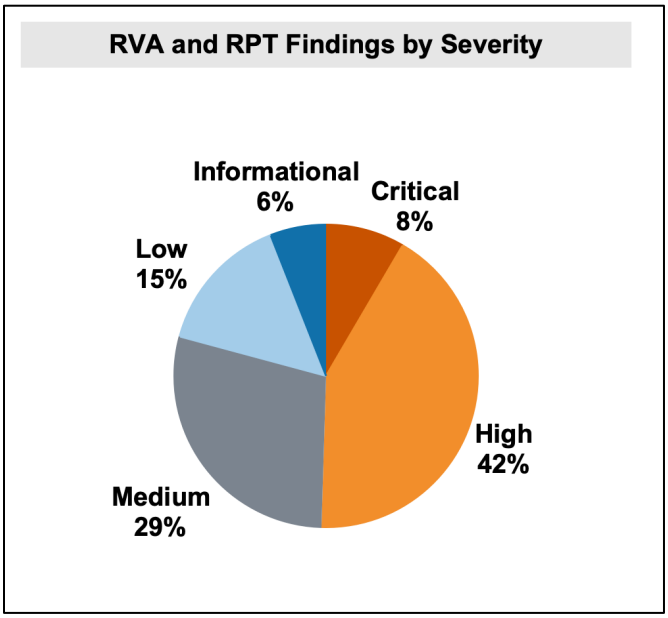

Figure 14: RVA and RPT Findings by Severity

CISA's findings are categorized by a severity schema described in more detail in Appendix B. The 8 percent critical-severity findings (55 out of 202) 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% high-severity findings (85 out of 202) indicate weaknesses or vulnerabilities that an adversary may be able to use to exercise full control on a target device if the vulnerability is exploited.

During the assessments, spearphishing weaknesses were the most common and successfully exploited (figure 15). The common 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 significant for all HPH entities to review and address, as many threat actors regularly initiate attacks by employing spearphishing to capture credentials and establish initial remote access.

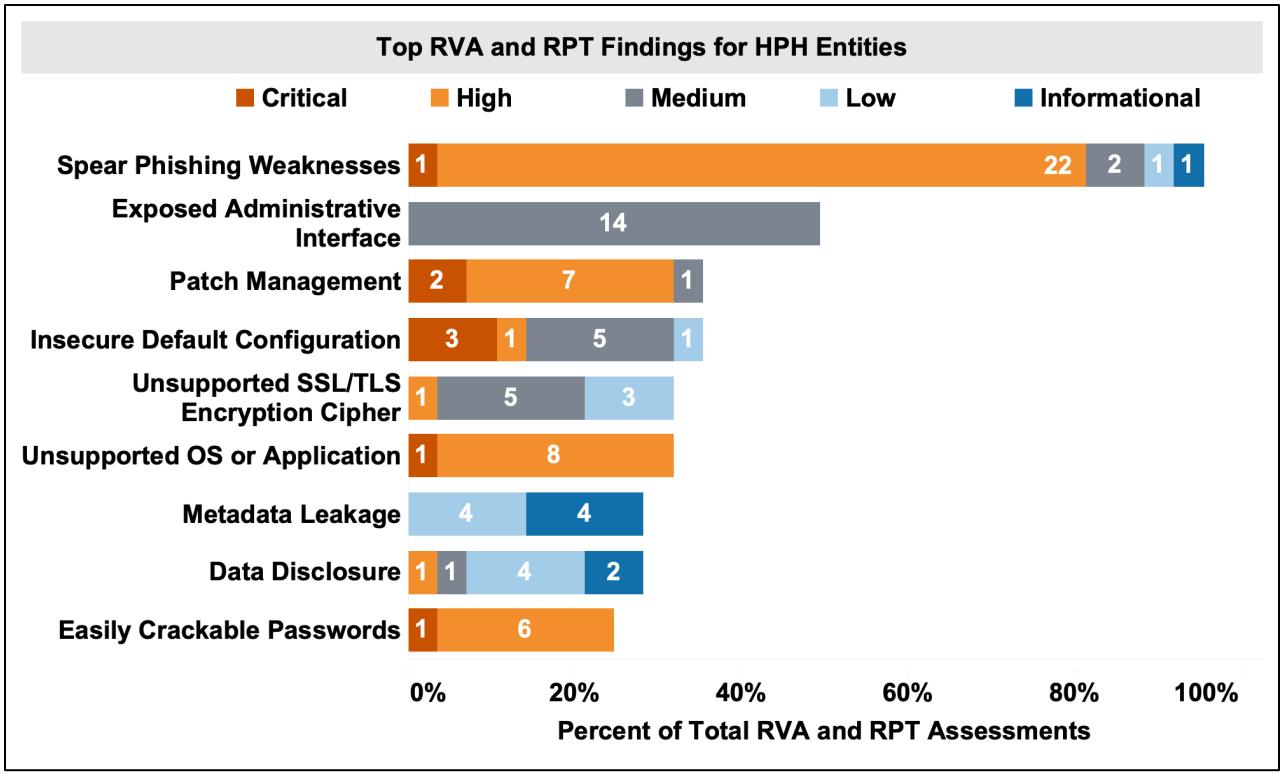

Figure 15: Top Findings from RVA Assessments in HPH Entities for FY 2019 and FY 2020

The next most frequent findings were exposed administrative interfaces and patch management (figure 15). Threat actors may be able to gain control of a network when administrative interfaces lack robust user authentication. Failing to apply the latest patches can leave the system open to attack with publicly available, widely known exploits. In both cases, the HPH entities could make it more difficult for adversaries to compromise their systems by patching systems and limiting access to administrative interfaces using access controls.

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 and 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 16).[18]

[18] 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**
Initial Access	Spearphishing Link	62.5%
	Valid Accounts	62.5%
Execution	Command-Line Interface	87.5%
Persistence	Valid Accounts	62.5%
Privilege Escalation	Valid Accounts	62.5%
Defense Evasion	Mshta	62.5%
	Process Hollowing	62.5%
	Valid Accounts	62.5%
Credential Access	Credential Dumping	62.5%
	Kerberoasting	62.5%
	LLMNR/NBT-NS Poisoning and Relay	62.5%
Discovery	Account Discovery	75.0%
	Network Service Scanning	75.0%
Lateral Movement	Pass the Hash	75.0%
Collection	Data from Network Shared Drive	62.5%
Command and Control	Commonly Used Port	75.0%
Exfiltration	Exfiltration Over Command and Control Channel	50.0%

Figure 16: Effective RVA Tactics and Techniques

Figure 16 provides tactics and techniques commonly used by adversaries to orchestrate attacks.

- *Phishing* [T1566] often provides the initial access point, followed by use of command-line interface (*Command and Scripting Interpreter* ([T1059]), *Valid Accounts* [T1078], *Mshta* [T1218.005], and *Processing Hollowing* [T1055.012]. All of these techniques allow an attacker to hide as a legitimate user while gaining privilege (*Privilege Escalation* [TA0004]) and evading defenses (*Defense Evasion* [TA0005]) on targeted systems. Command-line interface was used successfully in 87.5 percent of assessments to perform several actions, including data collection and *Execution* [TA0002] of code .
- Attackers use *OS Credential Dumping* [T1003] and *Pass-the-Hash* [T1550.002] to obtain credentials and passwords to access additional systems across the network (*Lateral Movement* [TA0008]).
- Attackers also leverage commonly used ports (*Application Layer Protocol* [T1071]) and *Exfiltration Over Command and Control Channel* [T1041] transfer to execute payloads (*Execution* [TA0002]) and exfiltrate data (*Exfiltration* [TA0010]) without alerting detection systems.
- Common themes noted across these techniques include nefarious use of tools in Windows platforms and masking nefarious 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 ratio of users who click on a phishing email—user click rate—and who interact with a potentially malicious email. The PCA allows phishing emails to bypass an entity's email 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. Across 30 campaigns, the click rate was 6.7 percent for HPH entities (figure 17), which is lower than the click rate for all PCAs CISA conducted in FY19 and FY20 (figure 18). However, although 6.7 percent might appear low, entities should understand that a single click on a phishing email can begin an attack chain leading to network compromise. Entities should continue efforts—such as training users and promoting awareness—to minimize this attack vector.

Phishing Campaign Assessment Findings for HPH 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
5	30	3,632	243	6.7%	56	1.5%	7:21 Minutes	11:51 Minutes

Figure 17: PCA Statistics for HPH Entities

Phishing Campaign Assessment Findings for all Critical Infrastructure

	Total Assessments	Total Campaigns	Emails Sent	Unique Clicks	Click Rate	User Reports	Report Rate	Average Time to First Click	Average Time to First Report
FY19	26	151	74,722	7,567	10.1%	2,660	3.6%	4:31 Minutes	19:51 Minutes
FY20	42	258	70,999	8,214	11.6%	5,263	7.4%	4:57 Minutes	4:03 Minutes

Figure 18: PCA Statistics for all Critical Infrastructure

An important counter-phishing method is training users on 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). HPH entities have a report rate of 1.5 percent compared to 7.4 percent report rate for all PCAs CISA conducted in FY20 (figures 17 and 18).

OBSERVATIONS, MITIGATIONS, AND BEST PRACTICES

The following recommendations and mitigations are based upon the analysis and findings of CISA vulnerability scanning and assessments outlined above. CISA provides these recommendations to help HPH entities reduce exposure to vulnerabilities and defend against threats. However, these recommendations do not guarantee protection against all cybersecurity risks impacting the HPH Sector. CISA encourages HPH 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. HPH Sector personnel were found to be susceptible to phishing attacks in PCAs; and separately, RVA and RPT teams were able to bypass email filtering controls to launch spearphishing in 96 percent of HPH assessments. In addition, PCAs for HPH entities had a 6.7 percent click rate and only a 1.5 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. HPH 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. [19,20] 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 assessments found the second most prevalent findings for HPH entities resulted from insufficient patch management. CISA scanning indicated that 69 percent of HPH entities experienced a critical or high vulnerability on at least one internet-accessible host during FY20. The median days to remediate vulnerabilities for HPH entities was 24.9 days for critical vulnerabilities and 57.6 days for high vulnerabilities. In addition, HPH entities' volume of active vulnerabilities per entity increased from 77 to 261 in FY20. Entities experiencing a growing vulnerability backlog over time increase the likelihood that one or more of those vulnerabilities are used as part of an attack.

Mitigation: Entities should seek to reduce the backlog of vulnerabilities, especially those with known exploits that could be used to breach the defensive perimeter. Entities should modify patch management strategies to prioritize patching critical vulnerabilities with proven exploits on high impact systems first and reduce time to remediate vulnerabilities.

Best Practice: Follow established enterprise network best practices for IT infrastructure, including the implementation of a strong patching methodology for OSs, applications, and firmware. Consider managing limited resources to patch vulnerabilities that present the most risk first, ranking prioritization by criticality, known exploits, and any threat-related information about specific vulnerabilities.

---

[19] 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.

[20] 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.

Unsupported Operating Systems

Observation: Threat actors target unsupported OS versions because the lack of security patches and updates increase the ease of exploitation. In Q4 of FY20, 54 percent of observed HPH entities had at least one internet-accessible host running an unsupported OS.

Mitigation: Entities should 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 replace equipment—including its software, firmware, OS, and hardware—that is no longer supported and isolate exceptions if replacement is not a viable option. [21]

Potentially Risky Services

Observation: Potentially vulnerable risky services, like FTP, Remote Procedure Call (RPC), and RDP, that are exposed to the internet present possible entry and escalation points for attackers. Throughout FY20, 50 percent of HPH entities scanned were running at least one risky service on an internet-facing 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 encryption through tunneling.[22]

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.

CONCLUSION

HPH 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. HPH entities are welcome to seek additional advice and assistance from CISA via vulnerability_info@cisa.dhs.gov and adopt additional healthcare cybersecurity best practices found in the HHS and Health Sector Coordinating Council joint publication, Health Industry Cybersecurity Practices (HICP).

Feedback regarding this product is critical to CISA's continuous improvement. CISA recently updated our anonymous product survey; we'd welcome your feedback

[21] NSA, Guidance on Eliminating Obsolete TLS Protocol Configurations. January 5, 2021. https://us-cert.cisa.gov/ncas/current-activity/2021/01/05/nsa-releases-guidance-eliminating-obsolete-tls-protocol.

[22] CISA Alert (AA20-073A) Enterprise VPN Security, Link: https://us-cert.cisa.gov/ncas/alerts/aa20-073a

APPENDIX A: POTENTIALLY RISKY SERVICES

Table 1: Most Common Potentially Risky Services Identified for Scanned HPH 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 cleartext, 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 communications over a non-secure network in a more secure manner. Unpatched Kerberos connection may allow a threat actor to authenticate onto an entity's network and 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 and 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 MFA used to secure access. Threat actors can use RDP to facilitate data theft and exposure, hijack login credentials, and execute 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 on database interfaces.
Telnet	Teletype Network (Telnet) is an application protocol used on the internet or local area network for unencrypted text communications and poses a severe security risk when exposed to the internet. 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. Examples include: • 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 detected; • Vulnerability that has tools readily available on the internet to take advantage of it; and • Weak passwords for remote administration and users.
Medium	Intruders may be able to exercise some control of the targeted device. Examples include: • 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; and • 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: PREVALENT RVA FINDINGS

Table 3: Most Prevalent RVA Findings for Scanned HPH 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 administrative interface is accessible without any form of authentication. This can allow unauthorized users to gain administrative privileges.	Properly restrict access to management and configuration interfaces and other potentially sensitive files on remotely accessible web servers, applications, and services. Use MFA for all administrative access.
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, network segmentation is highly recommended 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.
Insecure Default Configuration	Default configurations of systems, services, and applications can permit unauthorized access. Many off-the-shelf applications are released with built-in administrative accounts using predefined credentials that can often be found with a simple web search. As a result, an attacker with minimal technical knowledge can then use these credentials to access the related services.	Review all vendor applications and appliances. Verify the implementation of appropriate hardening measures and change, remove, or deactivate all default credentials.

Finding Name	Finding	Standard Remediation
Unsupported SSL/TLS Encryption Cipher	Use of an insecure SSL/TLS encryption algorithm. It is possible to implement SSL/TLS using many different encryption algorithms, and some are stronger and more secure than others.	Review all SSL/TLS encryption algorithms in use, and update any unsupported ciphers to versions compliant with applicable standards.
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. The overall security posture of the entire network is 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.
Metadata Leakage	Metadata can contain sensitive data related to security settings, owner username, storage directory, creation/modification dates, and even usernames and passwords associated with the data. Using publicly available tools, attackers can extract this metadata from files and obtain reconnaissance information to tailor further attacks against the target systems.	Strip metadata from all documents available via network-connected applications. Develop a process to verify the removal of sensitive data prior to publishing documents. Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.

Finding Name	Finding	Standard Remediation
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.
Easily Crackable Passwords	User account passwords on the system are common and widely used. An attacker can iterate through a wordlist to successfully predict the victim's password and gain access to the account.	Enforce user creation of strong/unique passwords in accordance with applicable federal standards, industry best practices, and/or organizational-defined requirements.