TLP:AMBER

CYBER RISK SUMMARY: EDUCATION FACILITIES SUBSECTOR

Publication: July 2021

Cybersecurity and Infrastructure Security Agency

TLP:AMBER

EXECUTIVE SUMMARY

This Cyber Risk Summary provides analysis, findings, and recommendations derived from non-attributable cybersecurity trends observed between January 1, 2020, and December 31, 2020, among Education Facilities Subsector entities enrolled in the Cybersecurity and Infrastructure Security Agency (CISA) Cyber Hygiene (CyHy) Vulnerability Scanning (VS) service (Appendix A).

CISA's analysis of the available data for scanned Education Facilities Subsector entities found:

- Education Facilities Subsector entities are likely vulnerable to threat actors who seek to exploit known critical and high vulnerabilities. These entities remediated critical severity vulnerabilities in **242.7** median days and high severity vulnerabilities in **215.3** median days, which likely indicates an extensive window of exposure to potential threat actor exploitation on internet-facing networks;
- **60**% of Education Facilities Subsector entities scanned via CyHy VS exposed risky services on internet-accessible hosts,[1] which can provide initial access and communication channels for command and control and data exfiltration, via exposed services like Remote Desktop Protocol (RDP);
- **53.3**% of entities ran unsupported Windows operating systems (OSs)[2] on at least one internet-accessible host at the end of Q4 of 2020, which further exposes entities to vulnerabilities that may enable compromise.

CISA recommends the following mitigations to reduce Education Facilities Subsector risk:

- Prioritize remediation of vulnerabilities using a risk-based approach that considers likelihood of attack, ease of exploitation, and the magnitude of probable impact.
- 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 legacy software and OSs to supported versions in a timely manner and within organizational constraints.

CISA encourages Education Facilities Subsector 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 Education Facilities Subsector entities for financial or politically motivated reasons. CISA also encourages Education Facilities Subsector entities to email vulnerability_info@cisa.dhs.gov for additional advice and assistance.

Note: If you have any feedback regarding this product, please fill out the CISA Product Survey.

[1] 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.

[2] Windows 7, Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008 are the only OSs considered unsupported in this analysis.

CONTENTS

INTRODUCTION

This Cyber Risk Summary aggregates and analyzes Education Facilities Subsector (hereafter, "Education")[3] data collected through CISA's CyHy VS service in 2020 (Appendix A). It provides insight into vulnerabilities on Education 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 Education entities and potentially disrupt national critical functions. CISA encourages Education 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 Education Subsector is a target for:

- Advanced persistent threats (APTs) backed by foreign governments that may seek to conduct espionage or disrupt U.S. critical functions and economic interests.
  - *Iran cybertheft campaign against hundreds of US universities (2018-2021)* [4]
  - *Chinese actors targeted universities for naval research (2019) and COVID-19 vaccine research (2020)* [5]
- Cybercriminals interested in profiting from data breaches and ransomware payments.
  - *Ransomware groups attacked multiple school districts (2021)*[6]

It is highly likely that the Education Subsector's increased use of new teaching technologies, networked devices, and remote learning during the COVID-19 pandemic expanded the Subsector's attack surface. According to industry reporting on global threat activity, as of June 2021, the Education Subsector faced more malware attacks than any other industry group.[7]

Threat actors leveraged the transition to remote learning by targeting school computer systems, slowing access, disrupting live-conferenced classroom settings, and launching ransomware attacks that compromise data and render systems inaccessible.[8] As of December 2020, the FBI, CISA, and the Multi-State Information Sharing and Analysis Center (MS-ISAC) observed multiple ransomware attacks against K-12 schools and higher education institutions.[9] Attackers are likely

[3] The Education Facilities Subsector consists of private and government-owned K-12 and higher education institutions.

[4] United States Department of Justice, Iranians Charged With Conducting Massive Cyber Theft. https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic

[5] https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800 ; https://www.cisa.gov/publication/fbi-cisa-psa-prc-targeting-covid-19-research-organizations

[6] Mississippi Today, Mississippi school districts targeted by ransomware attack. https://mississippitoday.org/2021/06/11/school-district-ransomware-attack-mississippi/ ; KENS5, Judson ISD recovering from ransomware attack, alert to district staff reveals. https://www.kens5.com/article/news/community/ransomware-attack-judson-isd-schools-satx/273-f2ccc437-bd45-4160-b5a4-945c46b1745e

[7] https://www.microsoft.com/en-us/wdsi/threats

[8] CISA, Cyber Threats to K-12 Remote Learning Education, https://www.cisa.gov/publication/cyber-threats-k-12-remote-learning-education

[9] CISA, Alert (AA20-345A) Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data. December 10, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-345a ; https://www.ic3.gov/Media/News/2021/210316.pdf

to use social engineering techniques, especially phishing, and exploit common vulnerabilities to gain initial access and steal or encrypt system data, according to industry reports.[10] Threat actors that infect systems with ransomware, not only disrupt the availability of those systems, but may also threaten to disclose sensitive student data, or sell information the darknet, if ransoms are not paid. It is almost certain that education entities will continue to be targeted as the attack surface expands to accommodate remote and hybrid learning. Education entities should evaluate the risk of exposure to cyber threats when maintaining and expanding their digital footprints and take steps to enhance their cybersecurity posture by proactively implementing mitigation strategies.

EDUCATION SUBSECTOR SAMPLE POPULATIONS

Over the course of 2020, Education Subsector participation in CyHy VS (Appendix A) increased by 56.8 percent with 359 total entities enrolled at the end of 2020. As enrollment continually expands, CISA discovers more hosts with active vulnerabilities within aggregated populations, such as other critical infrastructure sectors or subsectors.

CISA analyzed Education Entities that enrolled in CyHy VS prior to January 1, 2020:

- *229 entities*
- *254,519 hosts*

Trending analyses presented in this report control for and normalize the impact of continual enrollment by limiting the sample population during the period of analysis, January 1, 2020, to December 31, 2020. To eliminate the impact of observed fluctuations due to continuous enrollment, CISA evaluated 229 Education entities that enrolled and initiated scanning before January 1, 2020, for vulnerability findings and analysis. An additional, 130 Education entities that enrolled during 2020 are included in the analysis of prevalent vulnerabilities and potentially risky services.

VULNERABILITY SCANNING FINDINGS AND ANALYSIS

Vulnerability Severity Among Education Entities

Throughout 2020, CyHy VS scanning detected 125,141 total vulnerabilities on 254,519 hosts across 229 participating Education entities. Identified vulnerabilities were scored using the Common Vulnerability Scoring System (CVSS) version two (v2) base score:

- *2,174 (1.74 percent) were critical severity,*
- *6,399 (5.11 percent) were high severity,*
- *103,880 (83.01 percent) were medium severity, and*
- *12,688 (10.14 percent) were low severity.*

[10] Verizon, DBIR. https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/

Vulnerability Remediation

Median Days to Remediate

It is likely that critical and high vulnerabilities persisted, and will continue to persist, on Education entity networks for prolonged periods of time and increase the risk of compromise. Based on CISA's analysis of entities enrolled in CyHy VS, the median days to remediate[11] was 242.7 days for critical vulnerabilities and 215.3 days for high vulnerabilities. This means that the enrolled entities took more than 242.7 days and 215.3 days to remediate half of all remediated critical (1,385) and high (4,095) severity vulnerabilities, respectively. Sixty-one percent of Education entities with critical vulnerabilities remediated at least one critical vulnerability in under 43.0 days (25th percentile of remediation speed), suggesting the other 39 percent are likely faced with organizational challenges to remediating critical severity vulnerabilities in a timely manner. The Education Subsector's median days to remediate critical and high vulnerabilities was notably longer than other critical infrastructure and Federal Civilian Executive Branch (FCEB) entities (figure 1), which may suggest a lack of resources for some entities to effectively implement vulnerability management processes and continuously remediate vulnerabilities as they are disclosed.

2020 Median Vulnerability Remediation Time (in Days)

Severity	Education	Other CI	FCEB
Critical Severity	242.7	116.0	14.9
Critical Severity with Known Exploits	198.6	162.6	2.5
High Severity	215.3	93.9	8.3
High Severity with Known Exploits	145.5	120.7	8.1

***Only entities added prior to 2020 are considered in analysis.**

Figure 1: 2020 Median Remediation Timeframes

Median days to remediate can be impacted when Education entities attempt to address vulnerability backlogs.[12] For example, the median days to remediate critical severity vulnerabilities was likely extended due to Education entities that appropriately remediated long-standing critical vulnerabilities. However, extended remediation times—25 percent of remediated critical and high severity vulnerabilities were remediated in over 392.8 and 454.1 days respectively—suggest that some vulnerabilities persisted, and left entity networks exposed for over a year, significantly increasing cyber risk..

Education entities' remediation times may also be impacted by relying on specific operating systems (OSs), network protocols, and software that they are unable to upgrade, or alter without adversely impacting critical operations. This scenario prevents timely vulnerability remediation.

[11] Vulnerability management can be evaluated by examining the number of days between initial detection and remediation (when CyHy scanning no longer identifies the vulnerability on the host). The median number of days to remediate (or the middle value in the days to remediate data when sorted in order) provides a statistically robust indication of how long it takes entities to reduce their exposure to vulnerabilities.

[12] Vulnerability backlog is defined as the volume of active vulnerabilities an entity may possess within a timeframe.

For example, 65 Education entities remediated one Secure Sockets Layer (SSL) vulnerability[13] that accounted for 54.6 percent of all high severity vulnerabilities remediated in over 454.1 days, likely indicating that a few entities leveraged an insecure network protocol that may have provided threat actors with opportunities to degrade entities' data confidentiality and integrity for over a year. As entities remediate long-standing vulnerabilities, which is critical for reducing risk of compromise, they will likely see an increase in median days to remediate. A decrease will likely occur as an entity clears their vulnerability backlog and maintains a timelier remediation cadence.

It is likely that Education entities are struggling to maintain effective vulnerability management processes, based on analysis of remediation timeframes and vulnerabilities that remained active at year's end. At the end of 2020, 36.3 percent of critical severity and 36 percent of high severity vulnerabilities identified during the year were not remediated. This suggests that the volume of active vulnerabilities may be increasing and out-pacing capabilities to remediate, potentially providing threat actors increased opportunities to launch attacks. The prolonged exposure window or presence of vulnerabilities on Education entity networks likely makes them attractive targets for threat actors who seek to impact the confidentiality, integrity or availability of those networks.

> ***Strive to remediate critical and high vulnerabilities as quickly as possible.***
>
> *As a best practice—which is required for Federal Civilian Executive Branch (FCEB) agencies pursuant to federal directives—CISA strongly recommends remediating critical and high severity vulnerabilities on internet-accessible hosts within 15 and 30 days, respectively.*

Vulnerabilities with Known Exploits

Vulnerabilities with publicly available exploits are targeted by a wide array of adversaries because they require fewer resources and provide a higher probability of successfully accessing an entity's network. Entities should prioritize the remediation and mitigation of these vulnerabilities to limit their risk of an adverse cyber event. In 2020, the median days to remediate critical vulnerabilities with known exploits was 198.6 days, which likely indicates that vulnerabilities with known exploits persisted on Education Subsector networks for prolonged periods of time and increased their exposure and risk of compromise.

Exploit code or malware is developed for a small subset of vulnerabilities.[14] In 2020, CISA discovered that 7.3 percent of vulnerabilities across all severity categories on scanned internet-accessible Education Subsector networks had known exploits (figure 2). Although a small percentage of hosts may be impacted, critical severity and high severity vulnerabilities with known exploits significantly increase risk of exposure and should be prioritized for remediation. At the end of the fourth quarter (Q4) of 2020, 9.6% percent of scanned Education entities had critical severity vulnerabilities with known exploits on at least one host (figure 2). It is likely that 140

[13] "SSL Version 2 and 3 Protocol Detection" accounted for 54.6% of all high severity vulnerabilities remediated in over 454.1 days

[14] 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

Education entities with one medium severity SSL vulnerability[15] increased the percent of entities with vulnerabilities with known exploits throughout 2020.

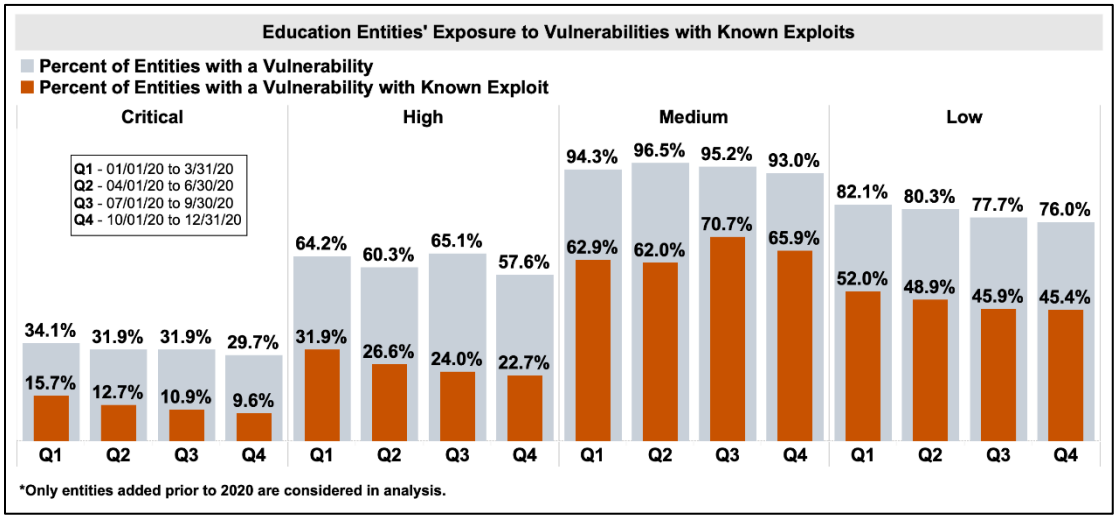

Figure 2: Education Entities' Vulnerabilities with Known Exploits

Medium and low severity vulnerabilities also have the potential to impact Education entities, as their presence on a network perimeter could become part of a chain of vulnerabilities used in 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.[16]

Vulnerabilities with known exploits are likely to be targeted by threat actors. Prioritizing remediation efforts on vulnerabilities with known exploits may help entities reduce the risk of compromise. For example, a highly prevalent, and publicly exploited vulnerability on an entity's high-value system may warrant a higher remediation priority than other vulnerabilities without known exploits. 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.[17]

[15] SSL Certificate Signed Using Weak Hashing Algorithm (CVE-2004-2761)

[16] 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.

[17] 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.

Active Vulnerabilities

During 2020, the number of active vulnerabilities per Education Subsector entity decreased by 16.4 percent, suggesting a reduction in exposure of internet-accessible vulnerabilities that may decrease the risk of compromise of Education entity networks (figure 3).

In 2020, entities that enrolled in CyHy VS reduced their active vulnerabilities by an average of 23.6 percent within the first three months

The average number of active vulnerabilities per entity provides insight into the Education Subsector's vulnerability management processes and how well the Subsector is doing in reducing existing vulnerabilities (figure 4). Remediating more vulnerabilities in a given month than the number of new vulnerabilities incurred provides a positive indication that an entity is keeping pace with or reducing active vulnerabilities.

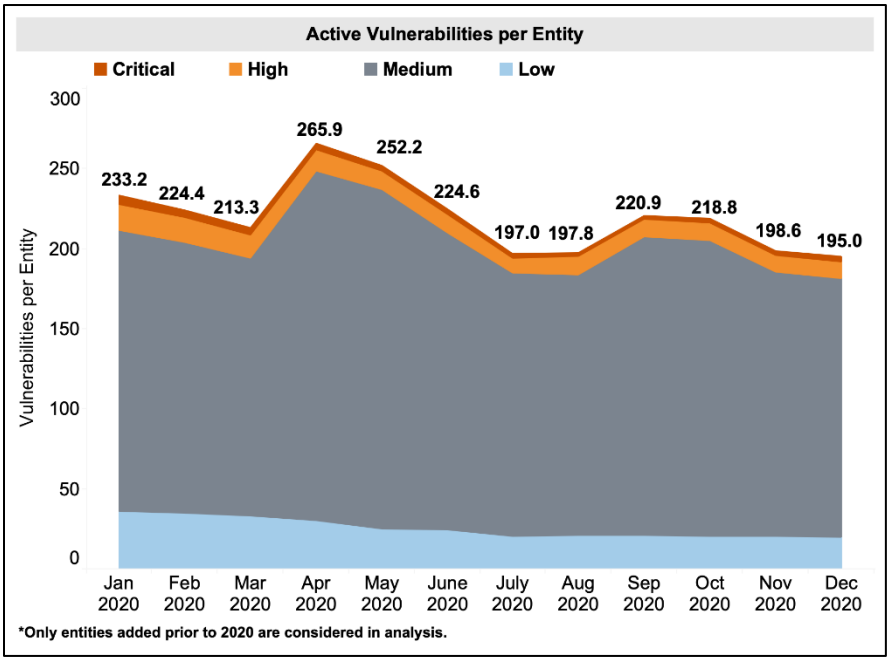

Figure 3: Active Vulnerabilities Per Education Entity

CISA identified prevalent medium vulnerabilities across the Education Subsector from March to April 2020 that almost certainly increased active vulnerabilities per entity by 24.7 percent in that timeframe. Major web browsers and vendors ceased support for Transport Layer Security (TLS) versions below 1.2, which likely contributed to the increase of active vulnerabilities per entity from March to April 2020.[18] The upgrading to supported TLS versions that occurred throughout the Subsector from April to December 2020 likely contributed to the overall decrease of active vulnerabilities per Education entity.

It is likely that with increased targeting during 2020, Education entities acted more urgently and prioritized vulnerability remediation efforts to reduce their cyber risk. The decrease in active

[18] CISA detected usage of TLS versions 1.0 and 1.1 that are likely deprecated. Tenable Plugin, TLS Version 1.0 Protocol Detection.

vulnerabilities—coupled with extended median days to remediate—suggests that Education entities must continue concerted efforts to reduce their vulnerability backlogs and overall exposure and risk of compromise.

Prevalent Vulnerabilities

CISA identified prevalent critical and high severity vulnerabilities in 2020 that likely highlight common issues across Education entities and hosts. The most prevalent vulnerability among the scanned Education Subsector entities was a high severity vulnerability for SSL Version 2 and 3 Protocol Detection (figure 4).[19] CISA recommends that all Education Subsector entities examine their ingress traffic for deprecated versions of SSL and TLS and work to remediate or mitigate this vulnerability. Usage of deprecated SSL or TLS Protocols may allow threat actors to gain access to sensitive information on Education entity networks.[20]

Most Prevalent Critical and High Vulnerabilities from CyHy VS

Vulnerability	Severity	Percent of Distinct Entities Affected	Percent of Distinct Hosts Affected
SSL Version 2 and 3 Protocol Detection	High	61.6%	0.74%
Unsupported Web Server Detection	High	47.1%	0.24%
PHP Unsupported Version Detection	Critical	25.1%	0.15%
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability (CVE-2019-11043)	High	24.8%	0.12%
Unix Operating System Unsupported Version Detection	Critical	22.3%	0.16%
Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities (CVE-2017-7679)	High	18.4%	0.06%
Apple Mac OS X Find-By-Content .DS_Store Web Directory Listing (CVE-2001-1446)	High	12.5%	0.03%
phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3) (CVE-2019-11768)	High	10.9%	0.04%
PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution (CVE-2012-1823)	High	10.3%	0.03%
PHP 5.6.x < 5.6.34 Stack Buffer Overflow (CVE-2018-7584)	High	9.7%	0.02%

*Percentages denoted in orange have known exploits available. Population actively scanned in 2020 includes 359 entities and 327,788 hosts.

Figure 4: Critical and High Vulnerabilities Detected by CyHy in 2020

[19] 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. SSL is an earlier version of the Transport Layer Security (TLS) cryptographic protocol.

[20] CISA, NSA Releases 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

Within the Education Subsector, it is likely that there is a high prevalence of out-of-date PHP and Apache software. This outdated software introduces vulnerabilities to entity networks, based on a CISA analysis of CyHy VS entities and a review of analysis from MS-ISAC.[21]

The top prevalent critical severity vulnerabilities (including those with known exploits) indicate that a number of hosts use unsupported software, protocols, and OS versions, which suggests Education entities may be struggling to replace unsupported legacy systems that can increase their risk of compromise.[22] Unsupported products provide threat actors an incentive to attack, as they can more easily exploit known weaknesses in these products to compromise networks and systems.

Entities and Hosts Running Unsupported Windows OS Versions

Unsupported OSs cannot be updated and introduce additional vulnerabilities that threat actors can exploit. CISA's identification of unsupported Windows OSs can indicate if an entity is exposed to additional vulnerabilities as vendors cease software security updates for unsupported products.

At the end of Q4 of 2020, CISA identified unsupported Windows OS versions (Windows 7, Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008) for 53.3 percent of scanned Education entities and 3 percent of scanned hosts (see Figure 5).[23] Throughout 2020, the percent of entities and hosts running unsupported Windows OS versions decreased, which likely indicates that Education entities are reducing their exposure to vulnerabilities due to unsupported Windows OSs.

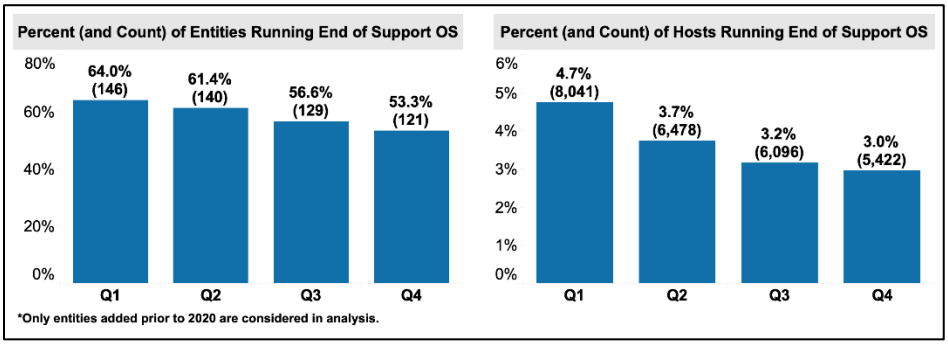

Figure 5: Education Entities and Hosts Running Unsupported OSs

Windows OSs are likely a subset of unsupported OSs used in the Education Subsector. Education entities should aim to reduce their use and dependence of all unsupported OSs on internet-accessible hosts. CISA encourages the Education entities to continue phasing out all unsupported OS versions within entity and vendor constraints and stay informed of end-of-support notifications.

[21] MS-ISAC Services. https://www.cisecurity.org/ms-isac/services/

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

[23] Hosts with unknown OS are factored into the overall hosts for the percentage calculation of unsupported OS versions.

Potentially Risky Services

CISA's CyHy VS helps monitor 10 potentially risky services that can increase an entity's risk of exposure to threats.[24] In 2020, 60 percent of scanned Education entities and 6.63 percent of their hosts were operating potentially risky services exposed to the internet (figure 6) that likely increase an entity's risk of exposure (see Appendix B). Although remote access services may be widely used in the Education Subsector to facilitate legitimate functionality and remote access to systems, they can increase risk if misconfigured or unprotected on internet-accessible hosts.

Education Subsector entities exposing Remote Desktop Protocol (RDP) and Server Message Block (SMB) services are likely to be targeted by threat actors, based on a review of MS-ISAC's 2020 port and service analysis from the Albert network monitoring service and CISA reporting of Russian APT activity and TrickBot malware activity tied to a cybercrime threat actor.[25,26]

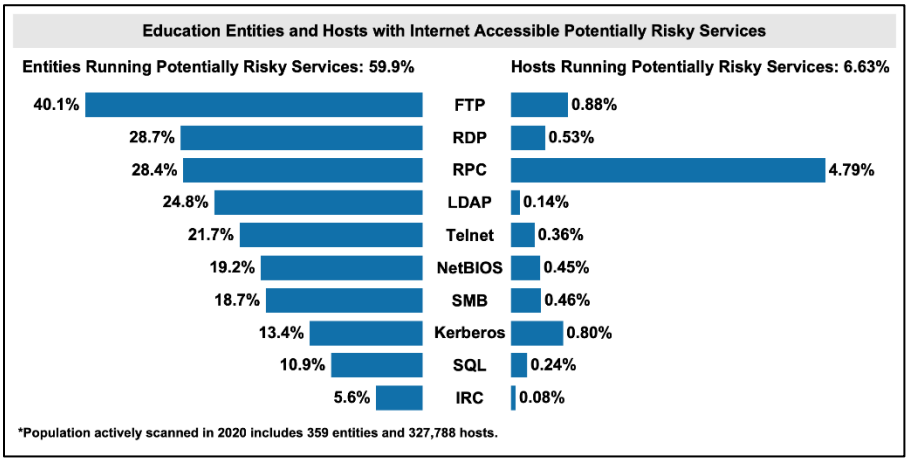

Figure 6: Education Entities and Hosts Running Risky Services on Open Ports

CISA also observed threat actors leveraging RDP—which allows remote connection to a computer over a network—to launch attacks against entities in multiple sectors, including the Education Subsector.[27,28] In 2020, 28.7 percent of Education entities ran RDP on at least one internet-accessible host. Due to the commonality of attacks involving RDP, entities using insecure RDP are susceptible to exploitation by threat actors who target RDP as part of their attack path. Remote access services like RDP are targeted by threat actors seeking initial access into systems.

---

[24] Services, also referred to as network and application protocols, allow devices to send information and communicate over private and public networks, including the internet. When exposed to the internet and unsecured, services are additional entry points for threat actors to launch and orchestrate remote attacks.

[25] As of May 20, 2021, CISA observed TrickBot laterally moving through entity networks by abusing SMB. TrickBot Malware | CISA

[26] Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets | CISA

[27] 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.

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

File Transfer Protocol (FTP) was the most prevalent potentially risky service, identified for 40.1 percent of entities; and Remote Procedure Call (RPC) was identified in 28.4 percent of entities and 4.8 percent of hosts (figure 6). RPC usage on Education hosts is 5.5 times higher than FTP, the most prevalent risky service based on analysis of entity usage. It is likely that extensive RPC usage on Education hosts may provide increased opportunities for adversaries who leverage RPC in their tactics and techniques for exploitation. It is likely that FTP services operated without secure encryption expose entities to threat actors who can steal sensitive data; and RPC can likely be leveraged by malicious actors to facilitate privilege escalation attacks.[29] Database services like Standard Query Language (SQL) may also be targeted by threat actors looking to steal sensitive information from exposed databases.

OBSERVATIONS, MITIGATIONS, AND BEST PRACTICES

The following recommendations and mitigations are based on the analysis and findings of the CISA vulnerability scanning outlined above. CISA provides these recommendations to help Education Subsector entities reduce exposure to vulnerabilities and defend against threats. However, these recommendations do not guarantee protection against all cybersecurity risks impacting the Education Subsector. CISA encourages Education 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.

Patch Management

Observation: Threat actors scan for and target vulnerable internet-accessible hosts to launch attacks. The median days to remediate vulnerabilities with known exploits for Education entities was 242.7 days for critical severity vulnerabilities and 215.3 days for high severity vulnerabilities. In addition, the average active vulnerabilities per Education entity decreased by 16.4 percent. Entities with smaller vulnerability backlogs over time may reduce likelihood that one or more of those vulnerabilities will be used as part of an attack.

Mitigation:

1. Regularly scan internet-accessible hosts and remediate critical and high severity vulnerabilities within 15 and 30 days, respectively.
2. Continue to reduce the backlog of vulnerabilities, especially those with known exploits that could be used to breach the defensive perimeter.
3. Prioritize remediation of vulnerabilities using a risk-based approach that considers likelihood of attack, ease of exploitation, and the magnitude of probable 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.[30]

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

[30] 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.

Implementation Resources:

Frameworks and Controls	Technical Guidance	Services
NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies	CISA: Ransomware Reference Materials for K-12 School and School District IT Staff	Sign up for CISA's Cyber Hygiene Vulnerability Scanning
NIST: Critical Cybersecurity Hygiene	CISA Insights: Understand Patches and Remediate Vulnerabilities for Internet-Accessible Systems	Use CISA's Detection and Prevention Services
DHS: Global Infrastructure for Managing Cybersecurity Vulnerabilities	CISA Insights: Secure Video Conferencing For Schools	CISA and CYBER.ORG "Cyber Safety Video Series" for K-12 students and educators

Potentially Risky Services

Observation: Threat actors seek to exploit certain services on entities' internet-accessible hosts to gain initial access to entity networks. Certain services like NetBIOS, Telnet, SMB, RDP, and others are vulnerable and often successfully exploited to deploy malware and move laterally throughout a network. Throughout 2020, 60 percent of Education entities scanned were running at least one potentially risky service on an internet-accessible host. Education entities using RDP and SMB are likely to be frequently targeted by threat actors, based on MS-ISAC's analysis.

Mitigation:

1. All listening network ports and services on a system should require a validated business reason to run. Entities should identify all internet-accessible services and secure or disable risky services according to the documented business reason for each service to operate.
2. In some cases, operating potentially risky services is necessary and can be accomplished by using additional security measures such as virtual private networks (VPNs), virtual network segmentation, secure credentials and MFA,[31] host-based and network-based firewalls, Transmission Control Protocol (TCP) wrappers or port access control list (ACL) measures, and prioritizing secure encryption.[32] It is important to note that many potentially risky services are unique and may require tailored risk assessments to determine an effective risk management approach.

[31] CISA Multifactor Authentication (MFA) Guidance, April 2021. https://www.cisa.gov/sites/default/files/publications/CISA MultiFactor Auth HDO_040721_508.pdf

[32] AA20-073A CISA Alert: Enterprise VPN Security..

Implementation Resources:

Frameworks and Controls	Technical Guidance	Services
Network Ports, Protocols, and Services: CIS Control 9; NIST CSF PR.IP-1 & DE.CM-8	NSA's guidance on Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations	Sign up for CISA's Cyber Hygiene Vulnerability Scanning
NIST Special Publication 800-39: Managing Information Security Risk	MS-ISAC's guidance on How to Restrict Server Message Block (SMB)	CISA's National Cybersecurity Assessments and Technical Services
NIST Special Publication 800-30: Guide for Conducting Risk Assessments	MS-ISAC's guidance on Remote Desktop Protocol (RDP)	Consider MS-ISACs Albert Network Monitoring service.

Unsupported Operating System Versions

Observation: Threat actors target unsupported OS versions because their lack of security patches and updates increases the ease of exploitation. At the end of Q4 of 2020, CISA identified unsupported operating systems for 53.3 percent of scanned Education entities and 3 percent of scanned hosts.

Mitigation:

1. Maintain a complete software asset inventory that includes the date when software and operating systems will no longer receive support.
2. Identify and plan to allocate resources to replace IT—including software, firmware, OSs, and hardware—that is no longer supported or will reach end-of-support in the near future.
3. For software or operating systems that are unsupported but are necessary to meet business needs, entities should document exceptions and implement mitigating controls such as network segmentation to isolate vulnerable systems.

Implementation Resources:

Frameworks and Controls	Technical Guidance	Services
Inventory and Manage Software Assets: CIS Control 2; NIST CSF ID.AM-2	MS-ISAC's End-of-Support Software Report List	CISA's Cyber Hygiene Services

CONCLUSION

Education Subsector 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 the standard cyber hygiene practices and applicable mitigations identified in this report to reduce their exposure. Education Subsector entities are welcome to seek additional advice and assistance from CISA via vulnerability_info@cisa.dhs.gov and adopt additional best practices[33] from the Research & Education Networks Information Sharing and Analysis Center (REN-ISAC).[34]

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] REN-ISAC Ransomware Guidance, Link: https://www.ren-isac.net/public-resources/Ransomware_Best_Practices.html

[34] REN-ISAC: Research Education Networking Information Sharing & Analysis Center

APPENDIX A: DATA COLLECTION METHODS AND SERVICES

Data from the following CISA service is analyzed in this report:

CyHy Vulnerability Scanning (VS) 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 CVSS version 2.0 scale of 0 to 10.[35] Nessus references the National Vulnerability Database (NVD) for its vulnerability information.[36] 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.

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

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

APPENDIX B: POTENTIALLY RISKY SERVICES

Table 1: Most Common Potentially Risky Services Identified for Scanned Education Subsector 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.