IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Cyber Risk Summary: Education Facilities Subsector

July 2021

FINDINGS

Cybersecurity and Infrastructure Security Agency (CISA) vulnerability management Cyber Hygiene Vulnerability Scanning performed between January 1, 2020, and December 31, 2020—identified the following vulnerabilities on Education entity IT assets. **Note:** This fact sheet uses data collected from Education Facilities Subsector entities as defined in the Government Facilities Sector Specific Plan. The Education Facilities Subsector consists of private and government-owned K-12 and higher education institutions.

Median number of **days to remediate critical and high** vulnerabilities was **242.7** and **215.3**, respectively

60% of entities ran at least one **risky service** on an **internet-accessible host**

53.5% of entities ran **unsupported Windows operating systems** on an **internet-accessible host**

MITIGATIONS

CISA recommends the following mitigations to reduce cyber risk among Education entities.

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: CISA recommends the following mitigations to improve patch management capabilities.

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. **Note:** See Carnegie Mellon University Software Engineering Institute's Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization for further guidance.

Potentially Risky Services

OBSERVATION: Threat actors seek to exploit certain services on internet-accessible hosts to gain initial access to entity networks. Certain services like NetBIOS, Telnet, Server Message Block (SMB), Remote Desktop Protocol (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: CISA recommends the following mitigations to avoid using potentially risky services.

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 multifactor authentication (MFA), host-based and network-based firewalls, Transmission Control Protocol (TCP) wrappers or port access control list (ACL) measures, and prioritizing secure encryption

Unsupported Operating System Versions

OBSERVATION: Threat actors target unsupported operating system (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: CISA recommends the following mitigations to reduce unsupported OS susceptibility.

1. Maintain 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 OSs 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

CISA recommends the following additional resources to help improve Education Facilities Subsector cybersecurity.

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
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

Frameworks and Controls	Technical Guidance	Services
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.
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

Note: *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.*