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

Cyber Risk Summary: Energy Sector

September 2021

FINDINGS

Cybersecurity and Infrastructure Security Agency (CISA) Cyber Hygiene Vulnerability Scanning (CyHy VS) performed between January 1, 2020, and December 31, 2020, identified the following vulnerability trends across 58 Energy Sector entities. The entities assessed for this summary may not be considered a representative sample of all Energy Sector entities in the United States. CyHy VS provides information on vulnerabilities found on internet-accessible IT systems and does not provide information on compensating controls that entities may employ to reduce the risk of compromise of previously identified or known vulnerabilities. Operational technology (OT) was not assessed or evaluated.

Remediated critical vulnerabilities **5 times faster** than other critical infrastructure sectors

45% of entities ran at least one **risky service** on an **internet-accessible host**

24% of entities ran **unsupported Windows operating systems** on an **internet-accessible host**

MITIGATIONS

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

Patch Management

OBSERVATION: Threat actors scan for and target vulnerable internet-accessible hosts to launch attacks. The median duration to remediate vulnerabilities for Energy entities was 25.3 days for critical severity vulnerabilities and 89.1 days for high severity vulnerabilities. In addition, average active vulnerabilities decreased by 4.4 percent per entity. Entities with fewer long-standing critical and high severity vulnerabilities may reduce their risk of compromise.

***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.*

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 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, 44.6 percent of Energy entities scanned were running at least one potentially risky service on an internet-accessible host.

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 OS versions because their lack of security patches and updates increases the ease of exploitation. At the end of 2020, CISA identified unsupported operating systems (OSs) for 24.1 percent of scanned Energy entities and 1.4 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 Energy Sector cybersecurity.

Frameworks and Controls	Technical Guidance	Services
NIST Special Publication (SP) 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 TLS Protocol Configurations	CISA's National Cybersecurity Assessments and Technical Services
NIST SP 800-39: Managing Information Security Risk	MS-ISAC's guidance on How to Restrict Server Message Block (SMB)	Consider MS-ISAC's Albert Network Monitoring service.
NIST SP 800-30: Guide for Conducting Risk Assessments	MS-ISAC's guidance on Remote Desktop Protocol (RDP)	
Inventory and Manage Software Assets: CIS Control 2; NIST CSF ID.AM-2	MS-ISAC's End-of-Support Software Report List	