CYBER RISK SUMMARY: ENERGY SECTOR

Publication: September 2021

Cybersecurity and Infrastructure Security Agency

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as TLP:AMBER: Limited disclosure, restricted to participants' organizations. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to. For more information on the Traffic Light Protocol, see https://www.us-cert.cisa.gov/tlp.

EXECUTIVE SUMMARY

CISA relies on your feedback to improve this product, please fill out the CISA Product Survey.

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 58 Energy Sector entities enrolled in the Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Hygiene (CyHy) Vulnerability Scanning (VS) service that identifies vulnerabilities on internet-accessible IT systems (Appendix A).

The vulnerabilities disclosed in this report are well-known and include mitigation measures. They have been shared broadly within the Energy Sector, along with mitigation measures, through CISA and the Energy Information Sharing and Analysis Center (E-ISAC). Enrolled Energy Sector entities may be aware of the identified vulnerabilities and may have implemented compensating mitigation measures that are not visible to CyHy VS scans.

CISA's analysis of the 58 Energy Sector entities found:

- Enrolled Energy Sector entities remediated critical vulnerabilities **5 times faster** than other critical infrastructure sectors with entities enrolled in CyHy VS.
- **45**% of enrolled Energy Sector entities scanned via CyHy VS expose services that can be risky when on internet-accessible hosts,[1] which can provide initial access points for threat actors to attempt exploitation through scanning exposed services like Remote Desktop Protocol (RDP). **Note:** entities with exposed services may be aware of the potential risks and may have implemented other mitigation measures.
- **24**% of enrolled Energy Sector entities ran unsupported Windows[2] operating systems (OSs) that no longer receive routine security updates on at least one internet-accessible host at the end of Q4 of 2020, increasing exposure to vulnerabilities that can enable compromise.

Based on the findings from the 58 scanned entities, CISA recommends all Energy Sector entities consider the following mitigations to reduce risk:

- Prioritize remediation of vulnerabilities using a risk-based approach that considers likelihood of attack, ease of exploitation, and the magnitude of probable impact.[3]
- 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 and policies.

[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.

[3] 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

Although the data used in this summary is not a representative sample of the whole Energy Sector, CISA encourages all Energy Sector entities to consider the findings and recommended mitigations in this summary 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 summary to disrupt national critical functions and target Energy Sector entities for financial or politically motivated crimes. CISA also encourages Energy Sector to email vulnerability_info@cisa.dhs.gov to enroll in CyHy VS or other services.

CONTENTS

Executive Summary 2

Introduction 5

Energy Sector Sample Population 6

Vulnerability Scanning Findings and Analysis 7

Vulnerability Severity Among Energy Entities 7

Vulnerability Remediation 7

Median Days to Remediate 7

Vulnerabilities with Known Exploits 9

Active Vulnerabilities 10

Prevalent Vulnerabilities 11

Entities and Hosts Running Unsupported Windows OS Versions 12

Potentially Risky Services 13

Observations, Mitigations, and Best Practices 14

Patch Management 15

Potentially Risky Services 16

Unsupported Operating System Versions 16

Conclusion 18

Appendix A: Data Collection Methods and Services 19

Appendix B: Potentially Risky Services 19

INTRODUCTION

This Cyber Risk Summary aggregates and analyzes enrolled Energy Sector entity data collected through CISA's CyHy VS service in 2020 (See Appendix A: Data Collection Methods and Services for more information on CyHy VS). This summary provides insight into vulnerabilities on 58 Energy Sector entities' scanned information technology (IT) assets and illustrates potential exposure to cyber threats. Operational technology (OT) was not assessed or evaluated. **Note:** this summary does not divulge the names of specific entities where CISA identified vulnerabilities.

Threat actors may actively leverage the weaknesses identified in this summary, based on the 58 scanned Energy Sector entities, to target Energy entities' IT assets that, if compromised, can indirectly affect OT systems and potentially disrupt national critical functions.[4, 5] CISA encourages Energy Sector entities to review the findings and recommended mitigations in this summary and evaluate their cybersecurity posture and capabilities, conduct further investigations, and prioritize actions to mitigate vulnerabilities and guard against threats.

The Energy Sector 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.
  - *Russian Government actors targeted the U.S. Energy Sector and other critical infrastructure sectors through a multi-stage intrusion campaign (2016 – 2018).*[6]
- Cybercriminals interested in profiting from data breaches and ransomware payments.
  - *To contain impacts from DarkSide ransomware, a U.S. pipeline system shutdown operations for several days. (2021)*
  - *A natural gas facility was impacted by ransomware that affected both IT and OT environments; however, the affected facility maintained control of operations during the incident. (2020).*[7]

According to U.S. Government reporting, the Energy Sector—which consists of the three interrelated Electric, Oil, and Natural Gas Subsectors—faces a multi-threat environment that includes combined cyber-physical attacks. Energy companies increasingly integrate their physical and cyber systems and install digital devices, such as smart meters and smart sensors, throughout their infrastructure.[8] If not properly configured and managed, interconnected IT and OT present an unknown risk of compromise that may result in significant cyber and physical impact.[9] Moreover, the sophistication of cybersecurity operations within energy companies ranges from very advanced to inadequate, based on U.S. Government reporting from 2018.[10]

[4] CISA, National Critical Functions (NCF). https://www.cisa.gov/national-critical-functions

[5] CISA Alert: AA21-131A, DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks. May 11, 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-131a

[6] CISA, Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. https://us-cert.cisa.gov/ncas/alerts/TA18-074A

[7] Ransomware Impacting Pipeline Operations | CISA

[8] DOE Multiyear Plan for Energy Cybersecurity | Department of Energy

[9] https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF

[10] DOE Multiyear Plan for Energy Cybersecurity | Department of Energy

Based on previous public, industry, and U.S. Government reporting on past cybersecurity attacks on the Energy Sector, it is almost certain that threat actors will use known attack vectors in continued attempts to compromise Energy Sector entities. These attack vectors include:

- Exploiting internet-accessible devices in IT and OT systems that include remote access capabilities,
- Supply chain attacks to compromise IT and OT assets, and
- Deploying spearphishing campaigns to gain initial access IT systems that may allow threat actors to pivot to OT networks.[11]

It is likely, based on industry reporting, that threat actors will continue to seek ways to deploy ransomware with OT-specific characteristics, such as EKANS, to disrupt operational technologies and demand higher payments.[12]

Previous attacks outside the United States, against foreign energy entities, demonstrated that attackers can perform unauthorized actions to cause loss of power, disrupt physical operating components, create a loss of visibility into operations, and create loss of productivity and revenue from downtime or ransomware payments.[13, 14] Successful attacks, with physical consequences, against U.S. Energy entities are highly likely to have significant financial costs and disrupt operations. These attacks could also have cascading consequences to other U.S. critical infrastructure (CI) sectors due to an almost universal dependence on electric power and fuel.[15] The information and mitigation strategies within this report can be used to prevent, or limit, the costs and negative impacts caused by cyberattacks.

ENERGY SECTOR SAMPLE POPULATION

CISA analyzed Energy entities that enrolled in CyHy vulnerability scanning prior to January 1, 2020:

- *58 entities*
- *6,246 hosts*

Over the course of 2020, Energy Sector participation in CyHy VS (Appendix A) increased by 27.6 percent, with 74 total entities enrolled at the end of 2020. To eliminate the impact of observed fluctuations due to continuous enrollment, CISA evaluated 58 Energy entities that enrolled and initiated scanning before January 1, 2020 for vulnerability findings and analysis. An additional, 16 Energy entities that enrolled during 2020 are included in analysis of prevalent vulnerabilities and potentially risky services. As CyHy VS enrollment across sectors continually expands, CISA discovers more hosts with active vulnerabilities within aggregated populations, such as a CI sector or subsector.

Findings produced from this analysis may be limited in their scope and generalizability. The 58 entities assessed for this summary may not be considered representative sample of all Energy Sector entities in the United States. Additionally, CyHy VS provides information on vulnerabilities

[11] https://www.gao.gov/assets/gao-21-81.pdf

[12] https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

[13] Cyber-Attack Against Ukrainian Critical Infrastructure | CISA

[14] https://www.wsj.com/articles/energy-tech-firm-hit-in-ransomware-attack-11620764034

[15] CISA, Energy Sector. https://www.cisa.gov/energy-sector

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.

VULNERABILITY SCANNING FINDINGS AND ANALYSIS

Vulnerability Severity Among Energy Entities

CyHy VS scanning detected 6,234 total vulnerabilities across 58 participating Energy entities and 6,246 hosts scanned throughout 2020. Identified vulnerabilities were scored using the Common Vulnerability Scoring System (CVSS) version two (v2) base score:[16]

- *6 (0.1 percent) were critical severity,*
- *205 (3.29 percent) were high severity,*
- *5,690 (91.27 percent) were medium severity, and*
- *333 (5.34 percent) were low severity.*

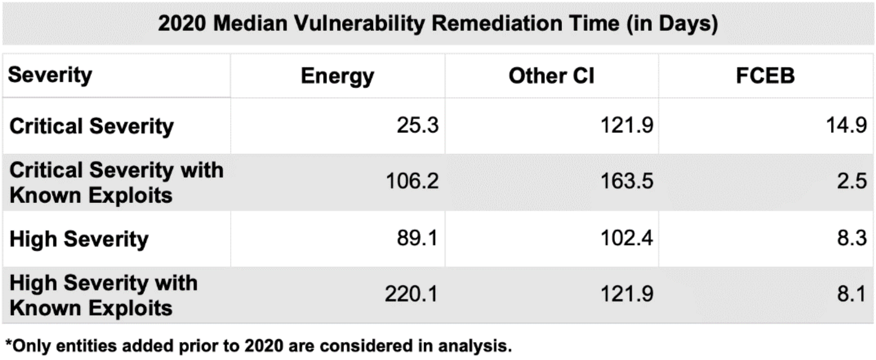
Vulnerability Remediation

Median Days to Remediate

Timely remediation of critical and high severity vulnerabilities likely reduces the risk of compromise. Enrolled Energy Sector entities remediated critical and high severity vulnerabilities on internet-facing assets faster than other CI sectors. Based on CISA's analysis of entities enrolled in CyHy VS, the median number of days to remediate[17] was 25.3 days for critical and 89.1 days for high severity vulnerabilities, meaning that half of all remediated critical and high severity vulnerabilities were remediated in greater than 25.3 and 89.1 days, respectively. 46.4 percent of Energy entities with at least one high severity vulnerability remediated them in under 19 days, which is within timeframe that CISA requires for federal agencies and a positive indicator of remediation speed. Meanwhile, other entities may face organizational challenges to remediate vulnerabilities in a timely manner. Based on CISA CyHy data holdings, the median days to remediate critical and high vulnerabilities for the Energy entities in this sample, was shorter than other scanned CI sectors combined and longer than Federal Civilian Executive Branch (FCEB) entities (Figure 1). This may suggest scanned Energy entities have more effective vulnerability management processes than other CI, however entities can further reduce windows of exposure to mirror FCEB entities that are directed to remediate critical and high severity vulnerabilities within 15 and 30 days respectively.

[16] CVSS v2 Complete Documentation (first.org)

[17] Vulnerability management can be evaluated by examining the number of days between initial detection and remediation (when CyHy scanning no longer identifies it 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.



2020 Median Vulnerability Remediation Time (in Days)

Severity	Energy	Other CI	FCEB
Critical Severity	25.3	121.9	14.9
Critical Severity with Known Exploits	106.2	163.5	2.5
High Severity	89.1	102.4	8.3
High Severity with Known Exploits	220.1	121.9	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 by a variety of factors, such as when entities attempt to address vulnerability backlogs.[18] For Energy Sector entities, median time to remediate vulnerabilities and addressing vulnerability backlogs may also be influenced by highly complex and geographically dispersed systems with zero ability for downtime that are likely more difficult and time consuming to remediate than other centralized IT systems. During 2020, the median days to remediate high severity vulnerabilities on IT systems was likely extended due to Energy entities appropriately remediating long-standing high severity vulnerabilities. However, extended remediation times, including the 25 percent of remediated high severity vulnerabilities whose remediation took over 372.8 days, mean that some vulnerabilities persisted, and, absent compensating controls, likely left entity networks exposed for over a year, increasing cyber risk.

Energy entities' remediation times may also be impacted by relying on specific operating systems, network protocols, and software that are unable to be upgraded, or altered without adverse impact to critical operations and as a result, prevent timely vulnerability remediation. For example, eight Energy entities remediated a Secure Sockets Layer (SSL) vulnerability in more than 89.1 days, adversely affecting high severity vulnerability remediation times. This indicates that a small number of 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. Over time, as this backlog is remediated and a timelier remediation cadence is implemented, entities will likely see a decrease in this metric.

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

Enrolled Energy entities did not remediate high severity as effectively as critical severity vulnerabilities, based on the analysis of vulnerabilities that remained active at year's end. At the end of 2020, 16.7 percent of critical severity and 43.9 percent of high severity vulnerabilities identified were not remediated. This might suggest that enrolled entities prioritized the remediation of critical severity vulnerabilities over high severity. If unaddressed, prolonged presence of vulnerabilities on Energy Sector networks almost certainly 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

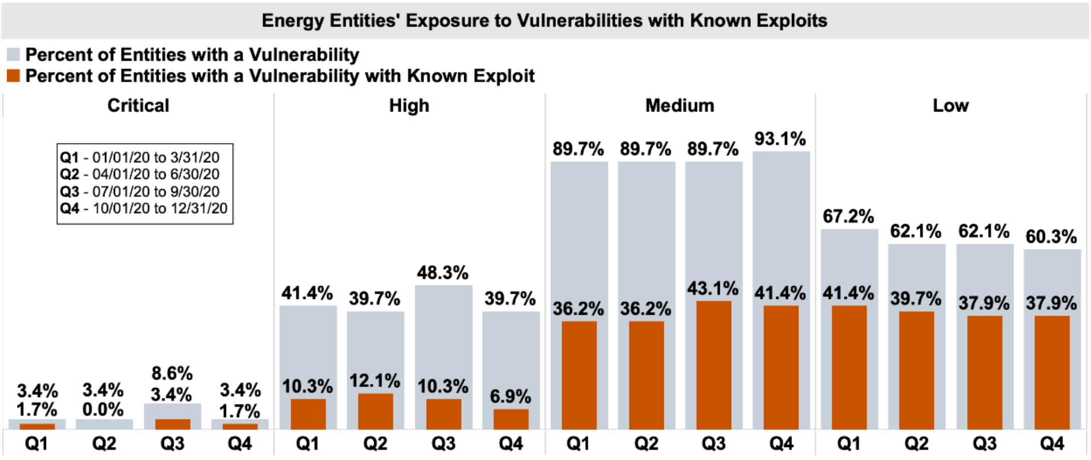
As a best practice—which is required for FCEB agencies pursuant to federal directives—CISA strongly recommends remediating critical and high severity vulnerabilities on internet-accessible hosts within 15 and 30 days, respectively.

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 the risk of an adverse cyber event. In 2020, enrolled Energy entities remediated five critical vulnerabilities, three of which had known exploits, and the median number of days to remediate critical vulnerabilities with known exploits was 106.2. This indicates that vulnerabilities with known exploits are persisting on Energy entity networks for prolonged periods of time; without the implementation of compensating controls, these vulnerabilities almost certainly increase the entities' exposure and risk of compromise.

Exploit code and malware are developed for a small subset of vulnerabilities.[19] In 2020, CISA discovered that 3.6 percent of vulnerabilities across all severity categories on scanned internet-accessible Energy Sector networks had known exploits (Figure 2). Critical severity and high severity vulnerabilities with known exploits significantly increase the risk of exposure and should be prioritized for remediation. At the end of the fourth quarter (Q4) of 2020, 1.7 percent of scanned Energy entities had critical severity vulnerabilities with known exploits on at least one host (Figure 2).

[19] 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



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

Figure 2: Energy Entity Vulnerabilities with Known Exploits

Medium and low severity vulnerabilities also have the potential to impact Energy 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.[20]

Vulnerabilities with known exploits are likely to be targeted by threat actors because they provide proven attack vectors for adversaries. Prioritizing remediation efforts on vulnerabilities with known exploits may help entities reduce risk of compromise. For example, 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.[21]

Active Vulnerabilities

During 2020, the number of active vulnerabilities per enrolled Energy Sector entity decreased by 4.4 percent, suggesting a slight reduction in exposure of internet-accessible vulnerabilities and risk of compromise of Energy Sector networks (Figure 3).

> *In 2020, entities that enrolled in CyHy VS increased their detection of active vulnerabilities by an average of 11.5 percent within the first three months.*

The average number of active vulnerabilities per entity provides insight into Energy Sector's vulnerability management processes and how well they reduce existing vulnerabilities (Figure 3).

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

[21] 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.

Remediation of more vulnerabilities than those that remain active in a given month provides a positive indication that an entity is keeping pace with or reducing active vulnerabilities.

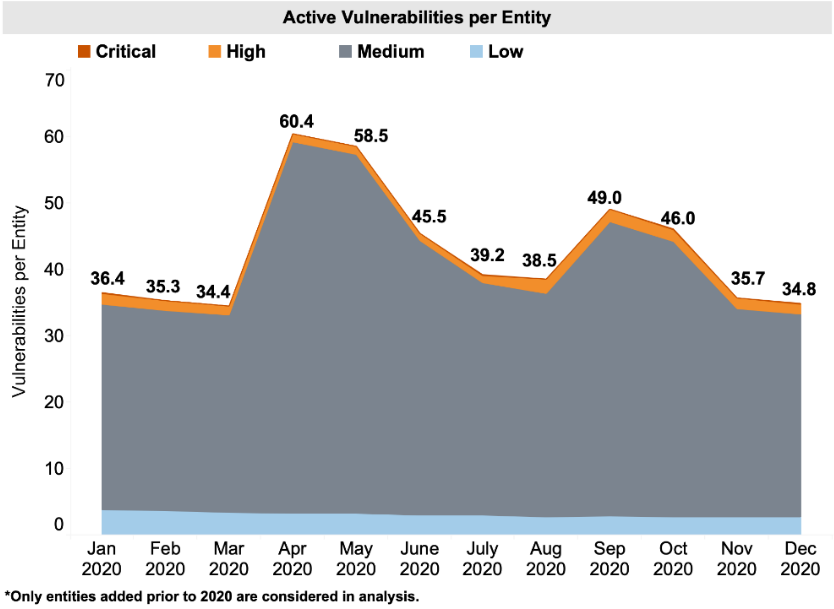


Figure 3: Active Vulnerabilities per Entity

CISA identified an influx of vulnerabilities across the Energy Sector from March to April 2020 that accelerated an increase of active vulnerabilities per entity in that timeframe. Major web browsers and vendors ceased support for TLS versions below 1.2, which likely contributed to the increase in active vulnerabilities per entity from March to April 2020.[22] Remediation of these TLS vulnerabilities from April to December 2020 likely contributed to the overall decrease of active vulnerabilities per entity.

It is likely that with increased targeting of other sectors, Energy entities acted more urgently and prioritized vulnerability remediation efforts to reduce their cyber risk. The decrease in active vulnerabilities—coupled with reduced median days to remediate—suggests that Energy entities must continue concerted efforts to reduce their vulnerability backlogs and overall exposure and risk of compromise.

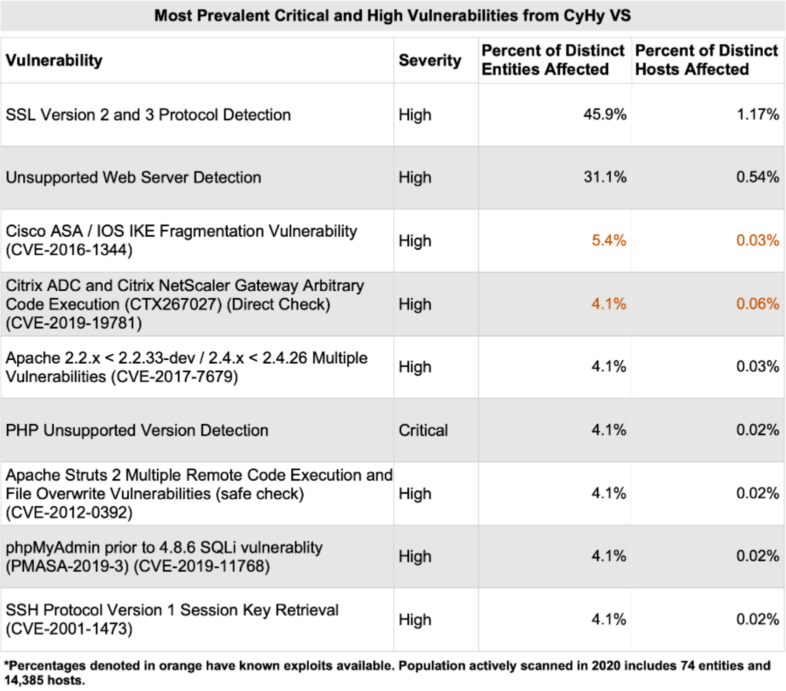
Prevalent Vulnerabilities

CISA identified prevalent critical and high severity vulnerabilities in 2020 that likely highlight common issues across Energy entities and hosts. The most prevalent vulnerability among the scanned Energy Sector entities was a high severity vulnerability for SSL Version 2 and 3 Protocol Detection (Figure 4).[23] CISA recommends that all Energy Sector entities examine their ingress

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

[23] 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.

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 Energy entity networks.[24]



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	45.9%	1.17%
Unsupported Web Server Detection	High	31.1%	0.54%
Cisco ASA / IOS IKE Fragmentation Vulnerability (CVE-2016-1344)	High	5.4%	0.03%
Citrix ADC and Citrix NetScaler Gateway Arbitrary Code Execution (CTX267027) (Direct Check) (CVE-2019-19781)	High	4.1%	0.06%
Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities (CVE-2017-7679)	High	4.1%	0.03%
PHP Unsupported Version Detection	Critical	4.1%	0.02%
Apache Struts 2 Multiple Remote Code Execution and File Overwrite Vulnerabilities (safe check) (CVE-2012-0392)	High	4.1%	0.02%
phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3) (CVE-2019-11768)	High	4.1%	0.02%
SSH Protocol Version 1 Session Key Retrieval (CVE-2001-1473)	High	4.1%	0.02%

***Percentages denoted in orange have known exploits available. Population actively scanned in 2020 includes 74 entities and 14,385 hosts.**

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

Within the Energy Sector, it is likely that there is a high prevalence of out-of-date PHP and Apache software, based on CISA's analysis of 58 Energy entities and a review of analysis from industry sources. This outdated software introduces vulnerabilities to entity networks that can lead to IT disruptions by denying access and allowing unauthorized code to be executed.[25]

The top prevalent critical and high severity vulnerabilities—SSL version detection, unsupported PHP, and web server detections—suggest that at least some Energy entities have not replaced unsupported legacy systems and deprecated network protocols that can increase their risk of compromise.[26] Unsupported products provide threat actors an opportunity to attack, and incentivize cyber criminals, 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 almost certainly introduce additional vulnerabilities that threat actors can exploit. CISA's identification of unsupported Windows OSs can indicate if an

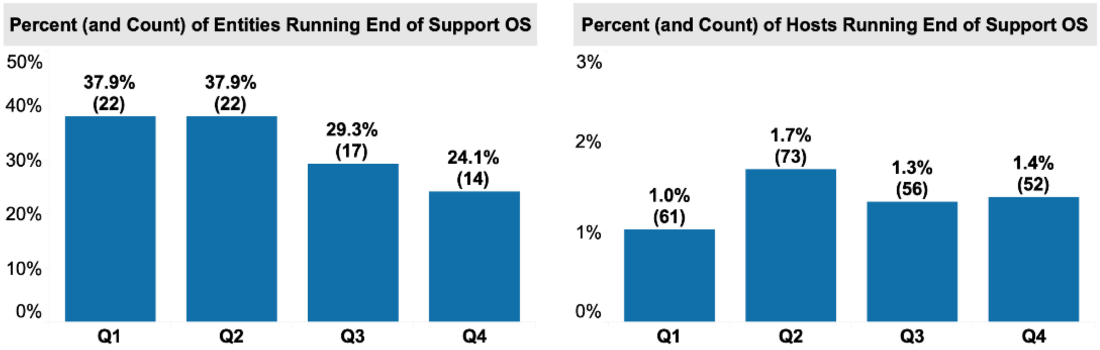
[24] CISA, NSA Releases Guidance on Eliminating Obsolete TLS Protocol Configurations, January 5, 2021. https://us-cert.cisa.gov/ncas/current-activity/2021/01/05/nsa-releases-guidance-eliminating-obsolete-tls-protocol

[25] PHP: List of security vulnerabilities (cvedetails.com)

[26] 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.

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 24.1 percent of scanned Energy entities and 1.4 percent of scanned hosts (see Figure 5).[27] Throughout 2020, the percent of entities running unsupported Windows OS versions decreased, while percent of hosts increased. It is likely that most entities are upgrading unsupported Windows OSs while a few are struggling to remove legacy Windows OSs from their internet-accessible IT infrastructure. Energy entities that are unable to upgrade or remove unsupported Windows OS will almost certainly have continued exposure and be at greater risk of compromise.


Percent (and Count) of Entities Running End of Support OS

Percent (and Count) of Hosts Running End of Support OS

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

Figure 5: Energy Entities and Hosts Running Unsupported OSs

It is likely that Windows OSs are a subset of all unsupported OSs used in the Energy Sector, and percent of entities and hosts that include other unsupported OSs may be higher. Entities should aim to reduce their use of, and dependence on, all unsupported OSs on internet accessible hosts. CISA strongly recommends that the Energy Sector continue phasing out all unsupported OS versions, within entity and vendor constraints, and stay informed of end-of-support notifications.

Potentially Risky Services

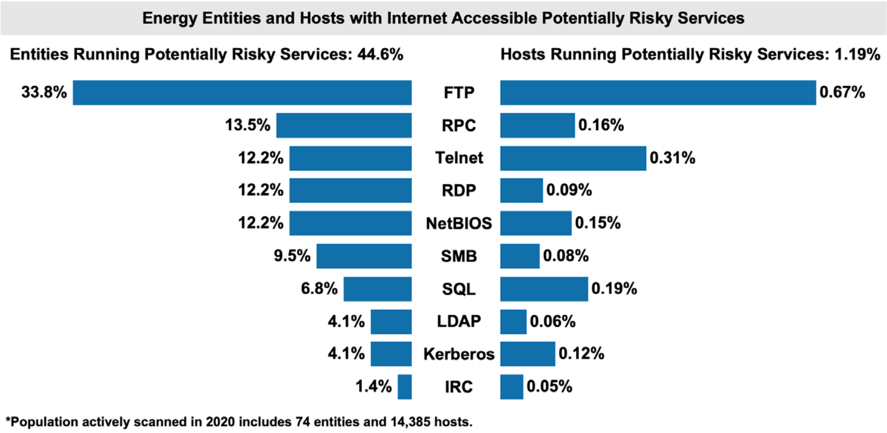
In 2020, 44.6 percent of scanned Energy entities and 1.19 percent of their hosts were operating potentially risky services exposed to the internet (Figure 6), according to CISA CyHy VS, which monitors 10 risky services[28] that likely increase an entity's risk of exposure (see Appendix B). Although remote access services may be used to varying degrees by entities within the Energy Subsectors—electricity, oil, and natural gas—to facilitate legitimate functionality and remote access to IT systems, they can increase risk if misconfigured or unprotected on internet-accessible hosts.

Remote Desktop Protocol (RDP) and Server Message Block (SMB) services are actively targeted by a variety of threat actors and across almost all critical infrastructure sectors, according to CISA

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

[28] 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.

and industry reporting. Any Energy Sector entity exposing RDP and SMB without monitoring or other compensating controls may increase the probability and likelihood of being targeted and compromised by threat actors who exploit these weaknesses.



Energy Entities and Hosts with Internet Accessible Potentially Risky Services

*Population actively scanned in 2020 includes 74 entities and 14,385 hosts.

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

In 2020, 12.2 percent of scanned Energy entities ran RDP on at least one internet-accessible host. CISA observed threat actors leveraging RDP–which allows remote connection to a device over a network–to launch attacks against entities from multiple sectors.[29, 30, 31] It is likely that entities using insecure RDP are susceptible to exploitation by adversaries due to the commonality of attacks involving remote services like RDP. Brute forcing unsecured RDP endpoints is among the most prevalent initial access vectors threat actors use to infect victims with ransomware.[32]

The most prevalent potentially risky services were File Transfer Protocol (FTP), identified in 33.8 percent of entities and Remote Procedure Call (RPC), identified in 13.5 percent of entities. It is likely that scanned entities operated FTP services without secure encryption, which exposes entities to threat actors who can steal sensitive data. RPC can likely be leveraged by malicious actors to facilitate privilege escalation attacks.[33] Database services like SQL, exposed by 6.8 percent of entities, 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

[29] 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.

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

[31] CISA, Alert AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks. July 08, 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-131a.

[32] FBI-CISA Joint Cybersecurity Advisory AA21-243A: Ransomware Awareness for Holidays and Weekends. August 31, 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-243a.

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

Energy Sector entities reduce exposure to vulnerabilities and defend against threats. However, these recommendations do not guarantee protection against all cybersecurity risks impacting the Energy Sector. CISA encourages Energy 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 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.

Mitigation:

1. CISA recommends regularly scanning internet-accessible hosts and remediating critical and high severity vulnerabilities within 15 and 30 days, respectively.
2. Entities should 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.[34]

Implementation Resources:

Frameworks and Controls	Technical Guidance	Services
Vulnerability Management: CIS Control 7; NIST CSF ID.RA-1	CISA's Recommended Practice: Patch Management of Control Systems	Sign up for CISA's Cyber Hygiene Vulnerability Scanning
NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies	CISA's Capacity Enhancement Guide: Remote Vulnerability and Patch Management	Use CISA's Detection and Prevention Services
Department of Energy's Cybersecurity Capability Maturity Model (C2M2) program	CISA Insights: Remediate Vulnerabilities for Internet-Accessible Systems	Reference E-ISAC's Cyber Incident Bulletins and ONG-ISAC's CISO Resources

[34] 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.

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:

1. All listening network ports and services on a system need 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),[35] host based and network-based firewalls, TCP wrappers or port ACL measures, and prioritizing secure encryption.[36] 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.

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-ISAC's Endpoint Detection and Response (EDR) 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

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

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

unsupported operating systems for 24.1 percent of scanned Energy entities and 1.4 percent of scanned hosts.

Mitigation:

1. Entities should maintain a complete software asset inventory that includes the date when software and operating systems will no longer receive support.
2. Entities should identify and plan to allocate resources to replace IT—including software, firmware, OSs, and hardware—that is no longer supported or scheduled to reach end-of-support.
3. For software or operating systems that are unsupported but are needed 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

Energy Sector entities can significantly reduce their cybersecurity risk by performing additional investigation and analysis of the findings described in this summary. CISA encourages entities to implement standard cyber hygiene practices and applicable mitigations identified in this summary to reduce their exposure. Energy entities are welcome to seek additional advice and assistance from CISA via vulnerability_info@cisa.dhs.gov and adopt additional best practices offered by the Electricity Information Sharing and Analysis Center (E-ISAC) and the Oil and Natural Gas Information Sharing and Analysis Center.[37]

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.

[37] E-ISAC Home (eisac.com) ; Information Center - ONG-ISAC (ongisac.org)

APPENDIX A: DATA COLLECTION METHODS AND SERVICES

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

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 Common Vulnerability Scoring System (CVSS) version 2.0 scale of 0 to 10.[38] Nessus references the National Vulnerability Database (NVD) for its vulnerability information.[39] 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.

APPENDIX B: POTENTIALLY RISKY SERVICES

Table 1: Most Common Potentially Risky Services Identified for Scanned Energy Sector 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

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

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

Service	Description
	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.