TLP:GREEN

Cyber Vulnerability Insights Estimate

Updated Analysis of Vulnerabilities Targeted by Iranian Government-Sponsored or -Linked Cyber Threat Actors

Scope: *This Cyber Vulnerability Insights Estimate (CVIE) contains analysis of common vulnerabilities and exposures (CVEs) that Iranian government-sponsored or -linked cyber threat actors have shown interest in, targeted, or successfully exploited according to threat reporting from the Cybersecurity and Infrastructure Security Agency (CISA), other U.S. government departments and agencies, foreign partners, and industry. Some exploitation activity dates back to 2012. These CVEs are referred to as "targeted CVEs" throughout this product. This CVIE is not an exhaustive list of targeted CVEs and does not rule out Iranian government-sponsored or -linked threat actor activity outside this period. The identification of CVEs in this CVIE does not constitute official U.S. government attribution of threat activity.*

Methodology and Limitations: *CISA derived CVE exposure data used in this CVIE from internet-accessible IT assets belonging to a sample of approximately 12,300 critical infrastructure entities enrolled in CISA Vulnerability Scanning and additional U.S. critical infrastructure entities visible through industry scan data from Dec. 8, 2025 to Feb. 9, 2026. Observed "instances" of a targeted CVE refer to any internet-accessible asset where at least one of the CVEs could be inferred from external scanning. This CVIE is an update to July 2025 CISA data, expanded threat research, and broader industry resources, offering a more thorough accounting of targeted CVEs than prior reports. This CVIE includes updated data from CISA Analysis in July 2025, with further threat research and expanded industry resources. This analysis does not account for possible compensating controls that entities may employ to reduce the risk of compromise of identified or known vulnerabilities.*

NATIONWIDE: Iranian government-sponsored or -linked cyber threat actors have previously targeted 136 CVEs; among these, 59 are present on critical infrastructure entities' internet-accessible networks.

CISA identified 136 unique CVEs that Iranian government-sponsored or -linked cyber threat actors have previously targeted and/or successfully exploited since 2012, based on an analysis of threat reporting from CISA, other U.S. government departments and agencies, foreign partners, and industry sources. Although these cyber threat actors often leverage brute force techniques or compromised credentials for initial access, these CVEs provide additional opportunities for initial access, lateral movement, and privilege escalation within victim networks.[1] The targeted CVEs span over 80 different software and hardware products provided by more than 50 vendors. Nearly 30% of these CVEs are associated with Microsoft software, predominately involving outdated or End-of-Service (EOS) versions of Windows and Exchange Server. Notably, a small number of common weakness enumerations (CWEs) is associated with a majority of the targeted CVEs and frequently appear across all critical infrastructure sectors. These overlapping vulnerabilities provide critical infrastructure organizations with the opportunity to significantly reduce risk from Iranian government-sponsored or -linked cyber threat actors by prioritizing remediation efforts on the most prevalent weaknesses. Over 30% of the 136 targeted CVEs are found in open source software (OSS), marking a 5% increase compared to CISA's CVIE analysis released July 2025. Of these, many are embedded in other products through software supply chains, including the three most widely exposed targeted CVEs (see Appendix A). Notably, in 2022, Iranian government-sponsored cyber threat actors exploited an OSS vulnerability to compromise a U.S. federal agency's network.[2]

[1] CISA, "Iranian Cyber Actors' Brute Force and Credential Access Activity Compromises Critical Infrastructure Organizations," October 16, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a.
[2] CISA, Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester," November 25, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-320a.

Table 1: Top Five Vendors With Products Most Frequently Associated With Targeted CVEs

Vendor	Products	Unique Targeted CVEs
Microsoft	Exchange Server Internet Explorer MSCOMCTL.OCX MSHTML Netlogon Office Remote Desktop Services SharePoint Win32k Windows Windows Server WordPad	**40 Total:** CVE-2010-0232 CVE-2012-0158 CVE-2014-4114* CVE-2015-1701 CVE-2016-0189 CVE-2017-0143 CVE-2017-0199 CVE-2017-0213 CVE-2017-11774 CVE-2017-11882 CVE-2018-8639 CVE-2019-0604 CVE-2019-0708 CVE-2020-0688 CVE-2020-1472 CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065 CVE-2021-31196 CVE-2021-31206 CVE-2021-31207 CVE-2021-33766 CVE-2021-33768 CVE-2021-34470 CVE-2021-34473 CVE-2021-34523 CVE-2021-34527 CVE-2021-40444* CVE-2022-30190* CVE-2022-30216 CVE-2023-29336 CVE-2024-30088 CVE-2024-49138* CVE-2025-21297* CVE-2025-21298* CVE-2025-21333* CVE-2025-21420* CVE-2025-53770* CVE-2025-9491*
WordPress	Multiple WordPress Themes, Plug-ins, and Modules	**9 Total:** CVE-2008-3362* CVE-2014-4725* CVE-2014-9735* CVE-2015-1579* CVE-2017-14723 CVE-2017-14726 CVE-2017-5611 CVE-2017-8295 CVE-2019-9879*
Apache	Log4j2 Tomcat RocketMQ	**6 Total:** CVE-2019-0232 CVE-2021-44228 CVE-2021-45046 CVE-2021-45105 CVE-2023-33246* CVE-2024-50379*
Fortinet	FortiOS FortiProxy RocketMQ	**6 Total:** CVE-2018-13379 CVE-2019-5591 CVE-2020-12812 CVE-2022-40684 CVE-2022-42475* CVE-2024-55591*
Ivanti/Pulse	Connect Secure Policy Secure ZTA Gateways	**5 Total:** CVE-2019-11510 CVE-2019-11539 CVE-2023-46805* CVE-2024-21887 CVE-2025-0282*

*Indicates newly added CVEs compared to CISA's CVIE analysis released July 2025

More than 3,100 U.S. critical infrastructure entities exposed nearly 67,000 total instances of internet-accessible assets vulnerable to targeted CVEs. Between Dec. 8, 2025 and Feb. 9, 2026, these entities collectively exposed 59 of the 136 (43%) unique CVEs targeted by Iranian government-linked cyber threat actors (see Appendix A). This represents a decrease from CISA's July 2025 analysis, which identified 54 of 90 (60%) targeted CVEs as exposed. Iranian government-linked cyber threat actors and aligned hacktivist groups often exploit targets of opportunity based on the exposure of unpatched or outdated software with known CVEs.[3]

[3] CISA, "Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest," June 30, 2025, https://www.cisa.gov/sites/default/files/2025-06/joint-fact-sheet-Iranian-cyber-actors-may-target-vulnerable-US-networks-and-entities-of-interest-508c-1.pdf.

Table 2: Targeted CVE Exposure by Sector

Sector	# of Targeted CVEs	Instances of Targeted CVEs	Unique Entities w/ Targeted CVEs
Information Technology	58	50,207	926
Communications	47	12,946	475
Commercial Facilities	39	630	266
Government Services and Facilities	37	942	493
Critical Manufacturing	33	370	206
Financial Services	30	597	168
Energy	29	203	107
Healthcare and Public Health	27	205	177
Food and Agriculture	26	93	65
Defense Industrial Base	21	211	19
Transportation Systems	20	121	96
Emergency Services	14	32	17
Water and Wastewater Systems	14	81	7
Chemical	13	45	22
Dams	1	3	1
Nuclear Reactors, Materials, and Waste	1	2	1

CISA observed an 80% overlap in the most prevalent targeted CVEs across all critical infrastructure sectors, representing an 11% decrease from the previous analysis. This continued overlap offers a substantial opportunity for risk reduction through focused remediation efforts. Furthermore, just seven CVEs account for the single most prevalent vulnerabilities across all 16 sectors individually (see Table 3). Key observations include:

- The dated "Heartbleed" OpenSSL vulnerability (CVE-2014-0160) was the most prevalent targeted CVE in five sectors between December 2025 and February 2026. Additionally, a deserialization vulnerability in Microsoft SharePoint (CVE-2025-53770) was the most prevalent in three sectors.
- A buffer overflow vulnerability (CVE-2022-42475) in Fortinet FortiOS ranked among the top 10 most prevalent CVEs in 13 sectors, the highest representation of any non-OSS product. Notably, industry threat reporting previously tied exploitation of this CVE to Fox Kitten and Pioneer Kitten, groups whose activities the U.S. government separately identified as being consistent with Iranian government-sponsored cyber threat actors.[4,5]
- Microsoft Exchange Server appeared most frequently in the top 10 list of most prevalent targeted CVEs across all sectors. CISA observed six Exchange Server CVEs in this list, including the commonly chained "ProxyLogon" CVEs. Government and industry reports documented exploitation of these vulnerabilities by various threat actors, including Mint Sandstorm, a group the U.S. government identified as an Iranian government-linked cyber threat actor.[6,7]

[4] Arctic Wolf, "Cybersecurity Risks Amid Rising Iran-U.S. Tensions," June 23, 2025, https://arcticwolf.com/resources/blog/cybersecurity-risks-amid-rising-iran-u-s-tensions/.
[5] CISA, "Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations," August 28, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a.
[6] Microsoft Threat Intelligence Center, "Evolving Trends in Iranian Threat Actor Activity," Microsoft, November 16, 2021, https://www.microsoft.com/en-us/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/.
[7] CISA, "Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society," May 14, 2025, https://www.cisa.gov/sites/default/files/2024-05/joint-guide-mitigating-cyber-threats-with-limited-resources-guidance-for-civil-society-508c_3.pdf.

Guidance on Microsoft Exchange and SharePoint

CISA urges critical infrastructure organizations to follow the updated guidance on Microsoft Exchange Server Security Best Practices that CISA and the National Security Agency (NSA) released in response to malicious exploitation activity against on-premises Exchange servers. Organizations can also reference CISA's Secure Cloud Business Applications (SCuBA) Project for secure baseline configurations that help harden Microsoft 365 Exchange Online, SharePoint, and other cloud applications against threat activity.

Table 3: Most Prevalent Targeted CVE per Sector

Sector	Most Prevalent Targeted CVE	Vendor/Product
Chemical	CVE-2017-14723	WordPress
Commercial Facilities	CVE-2022-42475	Fortinet FortiOS
Communications	CVE-2014-0160	OpenSSL
Critical Manufacturing	CVE-2024-6387	OpenSSH
Dams	CVE-2025-53770	Microsoft SharePoint
Defense Industrial Base	CVE-2022-42475	Fortinet FortiOS
Emergency Services	CVE-2016-10033	PHPMailer
Energy	CVE-2014-0160	OpenSSL
Financial Services	CVE-2014-0160	OpenSSL
Food and Agriculture	CVE-2017-14723	WordPress
Government Services and Facilities	CVE-2014-0160	OpenSSL
Healthcare and Public Health	CVE-2025-5777	Citrix NetScaler Application Delivery Controller (ADC) and Gateway
Information Technology	CVE-2024-6387	OpenSSH
Nuclear Reactors, Materials, and Waste	CVE-2025-53770	Microsoft SharePoint
Transportation Systems	CVE-2025-53770	Microsoft SharePoint
Water and Wastewater Systems	CVE-2014-0160	OpenSSL

More than half of all targeted CVEs were linked to previous ransomware activity, including multiple instances where Iranian government-sponsored or -linked cyber threat actors collaborated with ransomware operators and affiliates.[8] Since 2020, the U.S. government attributed ransomware activity to Iranian government-sponsored or -linked cyber threat actors on at least five separate occasions.[9] Such ransomware activity targeted U.S. government departments and agencies and multiple critical infrastructure sectors, including Communications, Defense Industrial Base, Education, Energy, Financial Services, Healthcare and Public Health, Government Services and Facilities, Information Technology, and Transportation Systems.

[8] CISA, "Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations," August 28, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a.
[9] CISA, "Iran State-Sponsored Cyber Threat: Advisories," Accessed February 23, 2026, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/iran/publications.

Iranian government-sponsored or -linked cyber threat actors repeatedly exploited Microsoft Exchange Server CVEs and vulnerabilities in network edge devices from Citrix, F5, Fortinet, and Ivanti/Pulse.[10, 11, 12, 13]

- CISA observed 43 of these ransomware-linked CVEs were exposed on the internet-accessible networks of at least 1,700 critical infrastructure entities as of Feb. 9, 2026, marking an increase of 5 CVEs and 600 entities since CISA's analysis in July 2025 (see Appendix A).

CISA's analysis of underlying security flaws across all targeted CVEs revealed 60 different CWEs, with the top five recurring CWEs accounting for nearly one-third of all vulnerabilities previously targeted by Iranian government-sponsored or -linked actors (see Table 4). Since 2019, MITRE has included these top five recurring CWEs in its annual list of the top 25 most dangerous software weaknesses.[14] Since CISA's analysis in July 2025, CISA identified additional instances of CWE-416 through further threat research and expanded prevalence scanning. Except for CWE-416, all of these CWEs are also included in the Open Web Application Security Program (OWASP) Foundation's top 10 most critical web application security risks.[15] CWE-22, covering vulnerabilities that enable directory/path traversal, was associated with both the largest number of targeted CVEs overall (12) and the highest number actively exposed (nine) by critical infrastructure entities.

Table 4: Top Five Recurring CWEs Among All Targeted CVEs

CWE	Underlying Vulnerability/Flaw	# of Targeted CVEs	In MITRE's 2025 Top 25 Most Dangerous Software Weaknesses?	In 2025 OWASP Top 10?
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12	Yes	Yes
CWE-502	Deserialization of Untrusted Data	9	Yes	Yes
CWE-20	Improper Input Validation	9	Yes	Yes
CWE-416	Use After Free	6	Yes	No
CWE-287	Improper Authentication	6	Yes	Yes

Critical infrastructure entities can reduce the risk of compromise by Iranian government-sponsored or -linked cyber threat actors through deliberate action. Focusing remediation efforts on the targeted CVEs that are most prevalently exposed on internet-accessible networks, such as the vulnerabilities identified earlier in Table 3, can drive substantial risk reduction across all critical infrastructure sectors. Additionally, CISA recommends organizations implement the following risk reduction measures as part of their organization's approach to cybersecurity:

- **Update or replace all devices exposing EOS operating systems, software, and protocols** and assume a breach until complete. All organizations should build a mature lifecycle management process, ensure isolation of any legacy business-critical operating systems or software until systems are replaced, and routinely monitor and investigate for signs of compromise.
- **Implement timely patch management** that prioritizes the remediation of known exploited vulnerabilities (KEVs) and targeted CVEs on internet-accessible assets. Follow up with threat hunting investigations to rule out prior compromise. Monitor CISA's KEV Catalog, Vulnerability Snapshots (TLP:GREEN), and CISA's cybersecurity advisories and alerts to maintain awareness of targeted CVEs and threat activity.

[10] CISA, "Iran-Based Threat Actor Exploits VPN Vulnerabilities," September 15, 2020, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-259a.
[11] CISA, "Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities," November 19, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-321a.
[12] CISA, "Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks," February 24, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-055a.
[13] CISA, "Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations," September 14, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-257a.
[14] MITRE, "CWE Top 25 Most Dangerous Software Weaknesses," February 10, 2025, https://cwe.mitre.org/top25/.
[15] OWASP Foundation, "OWASP Top 10:2025," November 6, 2025, https://owasp.org/Top10/2025/.

- **Secure cloud applications beyond default configurations.** See CISA's Secure Cloud Business Applications (SCuBA) Project and vendor-provided hardening instructions for guidance on strengthening the security and visibility of cloud environments.
- **Reduce the visible attack surface** through network segmentation and by disabling unnecessary product features and services. See CISA publications and joint guidance such as the Cross-Sector Cybersecurity Performance Goals (CPGs) and Sector-Specific Goals (SSGs).
- **Establish strong vendor risk management** including enhanced visibility into software supply chains. Consider CISA's Secure by Design principles when evaluating vendors and identify—using software bills of materials (SBOMs)—where and how vendor-provided products implement OSS.

APPENDIX A: TARGETED CVEs OBSERVED ON INTERNET-ACCESSIBLE NETWORKS

Key to acronyms for observed sectors:

CHEM=Chemical
CM=Critical Manufacturing
ES=Emergency Services
FA=Food and Agriculture
IT=Information Technology
NUC=Nuclear Reactors, Materials, and Waste
CF=Commercial Facilities
DAMS=Dams
ENRG=Energy
GSF=Government Services and Facilities
TS=Transportation Systems
COM=Communications
DIB=Defense Industrial Base
FS=Financial Services
HPH=Healthcare and Public Health
WWS=Water and Wastewater Systems

Table 5: Targeted CVEs and Associated Exposure on Internet-Accessible Networks

CVE ID	Vendor	Product	Instances	Unique Entities	Observed Sectors
CVE-2024-6387	OpenSSH	OpenSSH	14,116	786	CHEM, CF, COM, CM, DIB, ES, ENRG, FS, FA, GSF, HPH, IT, TS, WWS
CVE-2025-55182*	Meta	React Server Components	10,550	157	CF, COM, CM, ES, FS, FA, GSF, HPH, IT, TS
CVE-2014-0160	OpenSSL	OpenSSL	10,226	735	CHEM, CF, COM, CM, DIB, ES, ENRG, FS, FA, GSF, HPH, IT, TS, WWS
CVE-2025-53770*	Microsoft	SharePoint	4,198	250	CF, COM, CM, DAMS, DIB, ENRG, FS, FA, GSF, HPH, IT, NUC, TS, WWS
CVE-2018-6789*	Exim	Exim	3,662	165	CF, COM, CM, ENRG, FS, GSF, HPH, IT, TS
CVE-2022-42475*	Fortinet	FortiOS	3,556	701	CHEM, CF, COM, CM, DIB, ES, ENRG, FS, FA, GSF, HPH, IT, TS, WWS
CVE-2017-14723	WordPress	WordPress	3,257	488	CHEM, CF, COM, CM, DIB, ES, ENRG, FS, FA, GSF, HPH, IT, TS, WWS
CVE-2017-14726	WordPress	WordPress	2,350	357	CHEM, CF, COM, CM, DIB, ES, ENRG, FS, FA, GSF, HPH, IT, TS, WWS
CVE-2017-8295	WordPress	WordPress	2,165	337	CHEM, CF, COM, CM, DIB, ES, ENRG, FS, FA, GSF, HPH, IT, TS, WWS
CVE-2016-10033	PHP	PHPMailer	2,039	320	CHEM, CF, COM, CM, DIB, ES, ENRG, FS, FA, GSF, HPH, IT, TS, WWS
CVE-2024-50379	Apache	Tomcat	1,490	448	CF, COM, CM, DIB, ES, ENRG, FS, FA, GSF, HPH, IT, TS, WWS
CVE-2019-0708*	Microsoft	Remote Desktop Services	1,484	244	CHEM, CF, COM, CM, DIB, ENRG, FS, FA, GSF, HPH, IT, TS
CVE-2019-19781*	Citrix	ADC, Gateway, & SD-WAN WANOP Appliance	1,431	30	COM, CM, FS, IT
CVE-2017-5611	WordPress	WordPress	916	230	CF, COM, CM, DIB, ES, ENRG, FS, FA, GSF, HPH, IT, TS, WWS
CVE-2019-18935*	Progress	Telerik UI for ASP.NET AJAX	849	95	CHEM, CF, COM, CM, DIB, ENRG, FS, FA, GSF, HPH, IT, TS

CVE ID	Vendor	Product	Instances	Unique Entities	Observed Sectors
CVE-2022-36537*	ZK Framework	AuUploader	695	81	CF, COM, FS, HPH, IT
CVE-2024-41713*	Mitel	MiCollab	366	178	CHEM, CF, COM, CM, DIB, ES, ENRG, FS, FA, GSF, HPH, IT, TS
CVE-2019-11581	Atlassian	Jira Server & Data Center	348	84	CF, COM, CM, ENRG, FS, GSF, HPH, IT
CVE-2025-5777*	Citrix	NetScaler ADC & Gateway	285	240	CHEM, CF, COM, CM, ES, ENRG, FS, FA, GSF, HPH, IT, TS
CVE-2021-31206*	Microsoft	Exchange Server	268	189	CHEM, CF, COM, CM, DIB, ES, ENRG, FS, FA, GSF, HPH, IT, WWS
CVE-2019-0604*	Microsoft	SharePoint	265	151	CHEM, CF, COM, CM, ES, ENRG, FS, FA, GSF, HPH, IT, TS, WWS
CVE-2018-13379*	Fortinet	FortiOS	191	107	CF, COM, CM, DIB, ENRG, FS, FA, GSF, IT
CVE-2023-38950	ZKTeco	BioTime	182	37	COM, DIB, IT
CVE-2022-40684*	Fortinet	FortiOS, FortiProxy, FortiSwitch Manager	182	82	CF, COM, DIB, ENRG, FS, GSF, HPH, IT
CVE-2025-29927	Vercel	Next.js	156	28	COM, HPH, IT
CVE-2018-7600*	Drupal	Core	153	72	COM, ENRG, FS, GSF, IT, TS, WWS
CVE-2021-33766	Microsoft	Exchange Server	117	87	CF, COM, CM, ENRG, FA, GSF, HPH, IT, TS
CVE-2023-27350*	PaperCut	MF/NG	110	25	CF, COM, GSF, IT
CVE-2021-44228*	Apache	Log4j2	100	19	ENRG, GSF, HPH, IT, WWS
CVE-2021-34473*	Microsoft	Exchange Server	98	76	CF, COM, CM, ENRG, IT
CVE-2024-1709*	ConnectWise	ScreenConnect	90	36	COM, ENRG, IT
CVE-2021-31207*	Microsoft	Exchange Server	81	70	CF, COM, CM, ENRG, IT
CVE-2021-34523*	Microsoft	Exchange Server	81	70	CF, COM, CM, ENRG, IT
CVE-2024-57727*	SimpleHelp	SimpleHelp	77	42	CF, COM, IT
CVE-2021-26857*	Microsoft	Exchange Server	61	60	CF, COM, CM, DIB, FS, FA, GSF, IT
CVE-2021-26858*	Microsoft	Exchange Server	61	60	CF, COM, CM, DIB, FS, FA, GSF, IT
CVE-2021-26855*	Microsoft	Exchange Server	59	58	CF, COM, CM, DIB, FS, FA, GSF, IT
CVE-2021-27065*	Microsoft	Exchange Server	59	58	CF, COM, CM, DIB, FS, FA, GSF, IT
CVE-2024-24919*	Check Point	Quantum Security Gateways	51	35	COM, ENRG, IT
CVE-2019-0232	Apache	Tomcat	45	24	CF, COM, CM, ENRG, GSF, HPH, IT, TS
CVE-2022-21587*	Oracle	E-Business Suite	41	13	CF, GSF, HPH, IT
CVE-2023-46805*	Ivanti	Connect Secure & Policy Secure	32	30	COM, CM, FA, GSF, IT
CVE-2024-21887*	Ivanti	Connect Secure & Policy Secure	32	30	COM, CM, FA, GSF, IT
CVE-2019-5418	Rails	Ruby on Rails	21	9	GSF, IT
CVE-2019-11510*	Ivanti	Pulse Connect Secure	19	17	CF, COM, FS, HPH, IT
CVE-2019-11539*	Ivanti	Pulse Connect Secure & Pulse Policy Secure	16	12	CF, COM, GSF, IT
CVE-2023-33246	Apache	RocketMQ	8	6	IT

CVE ID	Vendor	Product	Instances	Unique Entities	Observed Sectors
CVE-2019-1579*	Palo Alto Networks	PAN-OS	7	6	CF, COM, IT
CVE-2020-5902*	F5	BIG-IP	7	6	COM, IT
CVE-2020-10188	netkit telnet	utility.c in telnetd	7	5	CF, COM, FA, GSF, IT
CVE-2021-26084*	Atlassian	Confluence Server & Data Center	6	5	CF, CM, IT
CVE-2023-0669*	Fortra	GoAnywhere MFT	5	2	IT
CVE-2022-1388*	F5	BIG-IP	4	2	IT
CVE-2020-1472*	Microsoft	Netlogon	3	3	IT
CVE-2024-53704*	SonicWall	SonicOS	3	3	COM, FS
CVE-2020-0688*	Microsoft	Exchange Server	2	1	IT
CVE-2023-47246*	SysAid	SysAid Server	2	3	IT
CVE-2021-21972*	VMware	vCenter Server	2	2	GSF, IT
CVE-2022-26134*	Atlassian	Confluence Server & Data Center	1	1	IT

*Indicates CVE is linked to previous ransomware activity according to CISA's KEV Catalog and industry threat reporting.

APPENDIX B: ADDITIONAL TARGETED CVEs

Table 6: Targeted CVEs With Zero Prevalence Among CISA's Critical Infrastructure Sample [16]

CVE ID	Vendor	Product
CVE-2023-26077	Atera	Atera Agent
CVE-2017-5963	Caddy	Caddy
CVE-2023-28130	Check Point	Gaia Portal
CVE-2023-28133	Check Point	Check Point Endpoint Security Client
CVE-2023-3519*	Citrix	NetScaler ADC and NetScaler Gateway
CVE-2024-8068	Citrix	Session Recording
CVE-2024-8069	Citrix	Session Recording
CVE-2024-10914	D-Link	Multiple Router Firmware
CVE-2024-12986	DrayTek	Vigor300B and Vigor2960
CVE-2019-5591*	Fortinet	FortiOS
CVE-2020-12812*	Fortinet	FortiOS
CVE-2024-55591*	Fortinet	FortiOS and FortiProxy
CVE-2024-21836	ggerganov	llama.cpp
CVE-2022-47986*	IBM	Aspera Faspex
CVE-2025-0282*	Ivanti	Connect Secure, Policy Secure, and ZTA Gateways
CVE-2019-0044	Juniper	Junos OS
CVE-2019-10068	Kentico	Xperience
CVE-2014-3931	Looking Glass	Multi-Router Looking Glass (MRLG)
CVE-2021-31196	Microsoft	Exchange Server
CVE-2021-33768	Microsoft	Exchange Server
CVE-2021-34470	Microsoft	Exchange Server
CVE-2025-9491	Microsoft	Windows
CVE-1999-0016	Multiple	Multiple
CVE-2015-8562	Open Source Matters	Joomla
CVE-2023-22047	Oracle Corporation	PeopleSoft Enterprise PeopleTools
CVE-2024-3400*	Palo Alto Networks	PAN-OS
CVE-2024-9474*	Palo Alto Networks	PAN-OS
CVE-2009-1151	phpMyAdmin	phpMyAdmin
CVE-2017-5930	PostfixAdmin	PostfixAdmin
CVE-2023-3539*	SimplePHPscripts	Simple Forum PHP
CVE-2019-9546	SolarWinds	Orion
CVE-2019-9621	Synacor	Zimbra Collaboration Suite (ZCS)
CVE-2024-45519	Synacor	Zimbra ZCS
CVE-2023-6448	Unitronics	Vision PLC and HMI
CVE-2022-22954*	VMware	Workspace ONE Access and Identity Manager
CVE-2008-3362	WordPress	Giulio Ganci Wp Downloads Manager Module 0.2
CVE-2014-4725	WordPress	MailPoet Newsletters

[16] CISA's Vulnerability Scanning results are not exhaustive for all CVEs and are not inclusive of all critical infrastructure entities. CISA strongly encourages all organizations to conduct their own vulnerability scanning to independently identify the presence of any targeted CVEs within their networks.

CVE ID	Vendor	Product
CVE-2014-9735	WordPress	ThemePunch Slider Revolution
CVE-2015-1579	WordPress	Elegant Themes Divi
CVE-2019-9879	WordPress	WPGraphQL 0.2.3
CVE-2015-4455	WordPress	Aviary Image Editor Add-on for Gravity Forms
CVE-2023-38951	ZKTeco	BioTime
CVE-2023-38952	ZKTeco	BioTime
CVE-2020-9054	Zyxel	Multiple Network-Attached Storage (NAS) Devices

*Indicates CVE is linked to previous ransomware activity according to CISA's KEV Catalog and industry threat reporting.