

News from Monday, January 29, 2024. Reported on Tuesday, January 30, 2024.

Live links are embedded throughout today's briefing. To see the actual URL, hover your mouse over the link for a moment before clicking. These links were copied directly from the web site of the source article. Tyler Cybersecurity has not performed any testing on the sites / links for security.

Sources	Articles
Bleeping Computer	Energy giant Schneider Electric hit by Cactus ransomware attack Energy management and automation giant Schneider Electric suffered a Cactus ransomware attack leading to the theft of corporate data, according to people familiar with the matter. BleepingComputer has learned that the ransomware attack hit the company's Sustainability Business division earlier this month on January 17th. The attack disrupted some of Schneider Electric's Resource Advisor cloud platform, which continue to suffer outages today. The ransomware gang reportedly stole terabytes of corporate data during the cyberattack and is now extorting the company by threatening to leak the stolen data if a ransom demand is not paid. While it is not known what type of data was stolen, the Sustainability Business division provides consulting services to enterprise organizations, advising on renewable energy solutions and helping them navigate complex climate regulatory requirements for companies worldwide. Customers of Schneider Electric's Sustainability Business division include Allegiant Travel Company, Clorox, DHL, DuPont, Hilton, Lexmark, PepsiCo, and Walmart. The stolen data could contain sensitive information about customers' power utilization, industrial control and automation systems, and compliance with environmental and energy regulations. It is not known if Schneider Electric will be paying a ransom demand, but if one is not paid, we will likely see the ransomware gang leaking the stolen data as they have done after previous attacks. In a statement to BleepingComputer, Schneider Electric confirmed that its Sustainability Business division suffered a cyberattack and that data was accessed by the threat actors. However, the company says the attack was restricted to this one division and did not impact other parts of the company. Keenan warns 1.5 million people of data breach after summer cyberattack Keenan & Associates is sending notices of a data breach to 1.5 million customers, warning that hackers accessed their personal information in a recent cyberattack. Keenan is a California-based insurance brokerage and consulting firm with an established presence in the education, healthcare, and public agencies sectors. Since 2017, it has been part of AssuredPartners NL, one of the largest brokerage firms in the U.S. The company submitted a notification to the Office of the Maine Attorney General, warning that 1,509,616 people were impacted by a data breach incident that occurred in the summer of 2023. "On Sunday, August 27, 2023, we discovered certain disruptions occurring on some Keenan network servers," reads the notification. "We immediately began an investigation and engaged leading third-party cybersecurity and forensic experts to assist."

Sources	Articles
	"The investigation determined that an unauthorized party gained access to certain Keenan internal systems at various times between approximately August 21, 2023 and August 27, 2023, and that the unauthorized party obtained some data from Keenan systems."
HIPAA Journal	<u>314,000 Patients Affected by Cyberattack on CompleteCare Health Network</u> CompleteCare Health Network, a health system serving patients in southern New Jersey, has recently confirmed that the protected health information of 313,973 patients has potentially been compromised in an October 2023 ransomware attack. An unauthorized third party gained access to certain CompleteCare Health Network computer systems and attempted to use ransomware to encrypt files. CompleteCare Health Network said this was a sophisticated ransomware attack that was detected and stopped on or around October 12, 2023. Third-party cybersecurity experts were engaged to investigate the attack and determine the nature of any unauthorized activity, and whether any patient data was involved. The substitute breach notice on the CompleteCare Health Network states, "Please know that we have taken steps to ensure your data will not be further published or distributed," which appears to confirm that there was data exfiltration, the threat group behind the attack threatened to publish the data, and payment was made to prevent that outcome. CompleteCare Health Network conducted a review of all files on the affected systems and confirmed they contained protected health information. The types of information involved varied from patient to patient and may have included names, phone numbers, addresses, and some sensitive personal information and/or personal health information. Notification letters started to be mailed to the affected individuals on December 15, 2023. Each individual notification letter states the exact types of data involved. CompleteCare Health Network said no reports have been received to indicate any actual or attempted misuse of patient data, but as a precaution, complimentary credit monitoring and identity theft protection services have been offered to the affected individuals. "Data security is one of our highest priorities. Upon discovering the incident, we immediately took the affected systems offline and began the process of securing and confirming the fortification of our systems," said a spokesperson for CompleteCare Health Network. Measures taken in response to the breach include revising policies and procedures and network security software, and reviewing how patient data are stored and managed. Since the attack, the network has been monitored 24/7 by third-party cybersecurity experts and CompleteCare Health Network has engaged leading cybersecurity firms to assist with monitoring its network for the long term. <u>Plaza Radiology Data Breach Affects Up to 569,000 Patients</u> Plaza Radiology, which does business as Chattanooga Imaging across several locations in Tennessee and North Georgia, has suffered a cyberattack and data breach that has affected up to 569,000 patients. Plaza Radiology identified the cyberattack on October 21, 2023, but did not disclose any details about the nature of the attack, other than stating that the initial results of the forensic investigation confirmed there had been unauthorized access to a small number of files on its network that contained patient information. The analysis of the results from the forensic investigation is ongoing and, at this stage, there have been no reports of any actual or attempted misuse of patient data. Plaza Radiology reported the data breach to the HHS' Office for Civil Rights on December 20, 2023, and said it will be mailing individual notification letters to the affected patients when the specific individuals affected have been identified and the types of data involved have been determined. Legal counsel for Plaza Radiology confirmed that several steps have been taken in response to the security breach to improve cybersecurity and prevent similar breaches in the future. Those measures include changing passwords on accounts, enabling multi-factor authentication, replacing the affected desktop computers and network servers, and providing enhanced security awareness training to the workforce.

Sources	Articles
	Plaza Radiology has confirmed that complimentary credit monitoring and identity theft protection services will be offered to individuals whose sensitive information was accessed in the attack and encourages all patients to be vigilant against identity theft and fraudulent uses of their data.
The Hacker News	<u>Malicious PyPI Packages Slip WhiteSnake InfoStealer Malware onto Windows Machines</u> Cybersecurity researchers have identified malicious packages on the open-source Python Package Index (PyPI) repository that deliver an information stealing malware called WhiteSnake Stealer on Windows systems. The malware-laced packages are named nigpal, figflix, telerer, seGMM, fbdebug, sGMM, myGens, NewGends, and TestLibs111. They have been uploaded by a threat actor named "WS." "These packages incorporate Base64-encoded source code of PE or other Python scripts within their setup.py files," Fortinet FortiGuard Labs said in an analysis published last week. "Depending on the victim devices' operating system, the final malicious payload is dropped and executed when these Python packages are installed." While Windows systems are infected with WhiteSnake Stealer, compromised Linux hosts are served a Python script designed to harvest information. The activity, which predominantly targets Windows users, overlaps with a prior campaign that JFrog and Checkmarx disclosed last year. "The Windows-specific payload was identified as a variant of the [...] WhiteSnake malware, which has an Anti-VM mechanism, communicates with a C&C server using the Tor protocol, and is capable of stealing information from the victim and executing commands," JFrog noted in April 2023. It's also designed to capture data from web browsers, cryptocurrency wallets, and apps like WinSCP, CoreFTP, Windscribe, Filezilla, AzireVPN, Snowflake, Steam, Discord, Signal, and Telegram.
Information Security Magazine	<u>Phobos Ransomware Family Expands With New FAUST Variant</u> Security researchers have recently uncovered a new variant of the notorious Phobos ransomware family named FAUST. Phobos, which first emerged in 2019, encrypts files on victims' computers and demands a ransom in cryptocurrency for the decryption key. According to an advisory published by FortiGuard Labs last Thursday, the FAUST variant was found in an Office document utilizing a VBA script to propagate the ransomware. As part of the campaign, the attackers employed the Gitea service to store malicious files encoded in Base64. When injected into a system's memory, these files initiate a file encryption attack. The FortiGuard Labs analysis revealed a multi-stage attack flow, from VBA script execution to the deployment of the FAUST payload. "Macros remain a dangerous part of malware delivery because VBA provides functionality that many companies use for day-to-day applications," explained John Bambenek, president at Bambenek Consulting. "The safest way to deal with this threat is to disable VBA in Office entirely. However, if that's not an option, organizations can at least disable 'high-risk' functionality in VBAs using Windows Defense Attack Surface Reduction, such as preventing office applications from creating child processes or from creating executable content."

Source	Article
CISA	Juniper Networks Releases Security Bulletin for J-Web in Junos OS SRX Series and EX Series Juniper Networks released a security bulletin to address multiple vulnerabilities for J-Web in Junos OS SRX Series and EX Series. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system. CISA encourages users and administrators to review the Juniper Bulletin JSA76390 and apply the necessary updates.

Source	Long Form Article
Dark Reading by Jai Vijayan (6 – 8 Minutes)	PoC Exploits Heighten Risks Around Critical New Jenkins Vuln Some 45,000 Internet-exposed Jenkins servers remain unpatched against a critical, recently disclosed arbitrary file-read vulnerability for which proof-of-exploit code is now publicly available. CVE-2024-23897 affects the built-in Jenkins command line interface (CLI) and can lead to remote code execution on affected systems. The Jenkins infrastructure team disclosed the vulnerability, and released updated version software, on Jan. 24. Since then, proof-of-concept (PoC) exploit code has become available for the flaw and there are some reports of attackers actively attempting to exploit it. On Jan. 29, the nonprofit ShadowServer organization, which monitors the Internet for malicious activity, reported observing around 45,000 Internet-exposed instances of Jenkins that are vulnerable to CVE-2024-23897. Nearly 12,000 of the vulnerable instances are in the US; China has almost as many vulnerable systems, according to ShadowServer data. Many enterprise software development teams use Jenkins to build, test, and deploy applications. Jenkins allows organizations to automate repetitive tasks during software development — such as testing, code quality checks, security scanning, and deployment — during the software development process. Jenkins is also often used in continuous integration and continuous deployment environments. Developers use the Jenkins CLI to access and manage Jenkins from a script or a shell environment. CVE-2024-23897 is present in a CLI command parser feature that is enabled by default on Jenkins versions 2.441 and earlier and Jenkins LTS 2.426.2 and earlier. "This allows attackers to read arbitrary files on the Jenkins controller file system using the default character encoding of the Jenkins controller process," the Jenkins team said in the Jan. 24 advisory. The flaw allows an attacker with Overall/Read permission — something that most Jenkins users would require — to read entire files. An attacker without that permission would still be able to read the first few lines of files, the Jenkins team said in the advisory. The vulnerability also puts at risk binary files containing cryptographic keys used for various Jenkins features, such as credential storage, artifact signing, encryption and decryption, and secure communications. In situations where an attacker might exploit the vulnerability to obtain cryptographic keys from binary files, multiple attacks are possible, the Jenkins advisory warned. These include remote code execution (RCE) attacks when the Resource Root URL function is enabled; RCE via the "Remember me" cookie; RCE through cross-site scripting attacks; and remote code attacks that bypass cross-site request forgery protections, the advisory said. When attackers can access cryptographic keys in binary files via CVE-2024-23897 they can also decrypt secrets stored in Jenkins, delete data, or download a Java heap dump, the Jenkins team said. Researchers from SonarSource who discovered the vulnerability and reported it to the Jenkins team described the vulnerability as allowing even unauthenticated users to have at least read permission

Source	Long Form Article
	on Jenkins under certain conditions. This can include having legacy mode authorization enabled, or if the server is configured to allow anonymous read access, or when the sign-up feature is enabled. Yaniv Nizry, the security researcher at Sonar who discovered the vulnerability, confirms that other researchers have been able to reproduce the flaw and have a working PoC. "Since it's possible to exploit the vulnerability unauthenticated, to a certain extent, it is very easy to discover vulnerable systems," Nizry notes. "Regarding exploitation, if an attacker is interested in elevating the arbitrary file read to code execution, it would require some deeper understanding of Jenkins and the specific instance. The complexity of escalation is dependent on the context." The new Jenkins versions 2.442 and LTS version 2.426.3 address the vulnerability. Organizations that cannot immediately upgrade should disable CLI access to prevent exploitation, the advisory said. "Doing so is strongly recommended to administrators unable to immediately update to Jenkins 2.442, LTS 2.426.3. Applying this workaround does not require a Jenkins restart." Sarah Jones, cyber-threat intelligence research analyst at Critical Start, says organizations using Jenkins would do well not to ignore the vulnerability. "The risks include data theft, system compromise, disrupted pipelines, and the potential for compromised software releases," Jones says. One reason for the concern is the fact that DevOps tools such as Jenkins can often contain critical and sensitive data that developers might bring in from production environments when building or developing new applications. A case in point occurred last year when a security researcher found a document containing 1.5 million individuals on the TSA's no-fly list sitting unprotected on a Jenkins server, belonging to Ohio-based CommuteAir. "Immediate patching is crucial; upgrading to Jenkins versions 2.442 or later (non-LTS) or 2.427 or later (LTS) addresses CVE-2024-23897," Jones says. As a general practice she recommends that development organizations implement a least-privilege model for limiting access and do vulnerability scanning and continuous monitoring for suspicious activities. Jones adds: "Additionally, promoting security awareness among developers and administrators strengthens the overall security posture."