News from Thursday, January 04, 2024. Reported on Friday, January 05, 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	**Ivanti warns critical EPM bug lets hackers hijack enrolled devices** Ivanti fixed a critical remote code execution (RCE) vulnerability in its Endpoint Management software (EPM) that can let unauthenticated attackers hijack enrolled devices or the core server. Ivanti EPM helps manage client devices running a wide range of platforms, from Windows and macOS to Chrome OS and IoT operating systems. The security flaw (tracked as CVE-2023-39336) impacts all supported Ivanti EPM versions, and it has been resolved in version 2022 Service Update 5. Attackers with access to a target's internal network can exploit the vulnerability in low-complexity attacks that don't require privileges or user interaction. "If exploited, an attacker with access to the internal network can leverage an unspecified SQL injection to execute arbitrary SQL queries and retrieve output without the need for authentication," Ivanti says. "This can then allow the attacker control over machines running the EPM agent. When the core server is configured to use SQL express, this might lead to RCE on the core server." The company says it has no evidence that its customers have been affected by attackers exploiting this vulnerability. Currently, Ivanti blocks public access to an advisory containing full CVE-2023-39336 details, likely to provide customers with more time to secure their devices before threat actors can create exploits using the additional information. **'everything' blocks devs from removing their own npm packages** Over the holidays, the npm package registry was flooded with more than 3,000 packages, including one called "everything," and others named a variation of the word. The package is quite aptly named as downloading "everything" will gradually pull in *every single npm package* that's ever been published to the npmjs.com registry onto your computer, potentially making it run out of storage. But that's just the tip of the iceberg. Since these 3,000+ packages manage to *include* every single npm package on the npmjs.com registry as their dependency, npm package authors who have ever published to the npm registry would now be unable to remove their packages at will, because of npm's policy. Installing *everything* could have just caused your computer to potentially fall short of storage space and slow down, but the package's mere existence on npmjs.com prevents authors—unrelated to this package whatsoever, from unpublishing their packages from the world's largest JavaScript software registry. The "everything" package has just 5 sub-packages, published under the "@everything-registry" scope, listed as its dependencies, BleepingComputer has observed. Considering the author of "everything" has published 3,000 plus such packages (chunks), each with hundreds of dependencies, a single `npm install everything` command will start resolving, what's referred to as transitive dependencies, and end up downloading millions of packages.

Sources	Articles
HIPAA Journal	**Integris Health Facing Multiple Class Action Lawsuits Over Cyberattack** Several class action lawsuits have been filed against Integris Health over its recent cyberattack and data breach. While Integris Health has yet to confirm how many individuals have been affected, the threat actor behind the attack claims to have obtained the data of around 2 million patients and emailed those patients directly on December 24, 2023, demanding payment after Integris Health refused to pay the ransom. Federman criticized Integris Health for the lack of transparency about the cyberattack and data breach, claiming Integris Health did not make any announcement about the attack until after patients were contacted directly by the hackers. Integris Health explained in its notification to patients that the threat actor gained access to its systems on November 28, 2023. Federman alleges Integris Health withheld important information that could have allowed the plaintiff and class members to take action to secure their identities and protect against fraud. While it is typical for healthcare organizations to offer complimentary credit monitoring and identity theft protection services when sensitive data is known to have been stolen, those services do not appear to have been offered. Integris Health, the largest not-for-profit Oklahoma-owned health system in the state, has confirmed that its internal systems have been compromised in a cyberattack and an unauthorized third party obtained patient data. Integris Health operates 15 hospitals in Oklahoma and many specialty clinics, family care practices, and centers of excellence. Integris Health uploaded a notice to its website on December 24, 2023, about a data privacy incident. According to Integris Health, suspicious activity was detected within its IT systems, and immediate action was taken to prevent further unauthorized access. An investigation was launched to determine the nature and scope of the breach, which revealed the unauthorized access started on November 28, 2023. The unauthorized actor exfiltrated sensitive data from Integris Health's systems but did not encrypt files. Integris Health has conducted a review of the affected files and has confirmed that the compromised information includes names, dates of birth, contact information, demographic information, and Social Security numbers. Integris Health said health information, financial information, driver's licenses, and usernames/passwords were not stolen. On December 24, 2023, Integris Health started to be contacted by some of its patients after they received communications from a group that claimed responsibility for the cyberattack. The threat group explained in the communications with patients that they had obtained names, dates of birth, SSNs, addresses, phone numbers, insurance information, and employer information, and that they would be selling the data on the dark web to be used for fraud and identity theft. Patients were told they could prevent the sale of their data by making a payment before January 5, 2024, otherwise, the entire database will be sold to a data broker. The communications with patients include a sample of the stolen data as proof, which some patients have confirmed is genuine. The threat actor claims to have obtained the protected health information of more than 2 million Integris Health patients, and that the reason for demanding payment from patients is because Integris Health has refused to pay to have the information deleted. The patients have been provided with a Tor link to make payment and the threat actor is charging individuals $3 to view their stolen data or $50 to have the data deleted. According to Bleeping Computer, the Tor extortion site lists 4,674,000 records, although it is unclear if all those records are unique. Integris Health has yet to confirm how many individuals have been affected.
The Hacker News	**UAC-0050 Group Using New Phishing Tactics to Distribute Remcos RAT** The threat actor known as UAC-0050 is leveraging phishing attacks to distribute Remcos RAT using new strategies to evade detection from security software. "The group's weapon of choice is Remcos RAT, a notorious malware for remote surveillance and control, which has been at the forefront of its espionage arsenal," Uptycs security researchers Karthickkumar Kathiresan and Shilpesh Trivedi said in a Wednesday report. "However, in their latest operational twist, the UAC-0050 group has integrated a pipe method for interprocess communication, showcasing their advanced adaptability."

Sources	Articles
	Over the past few months, the same trojan has been distributed as part of at least three different phishing waves, with one such attack also leading to the deployment of an information stealer called Meduza Stealer. The LNK file in question collects information regarding antivirus products installed on the target computer, and then proceeds to retrieve and execute an HTML application named "6.hta" from a remote server using mshta.exe, a Windows-native binary for running HTA files. The binary also employs unnamed pipes to facilitate the exchange of data between itself and a newly spawned child process for cmd.exe to ultimately decrypt and launch the Remcos RAT (version 4.9.2 Pro), which is capable of harvesting system data and cookies and login information from web browsers like Internet Explorer, Mozilla Firefox, and Google Chrome.

Source	Article
CISA	**CISA Releases Three Industrial Control Systems Advisories** CISA released three Industrial Control Systems (ICS) advisories on January 4, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS. • ICSA-24-004-01 Rockwell Automation FactoryTalk Activation • ICSA-24-004-02 Mitsubishi Electric Factory Automation Products • ICSA-23-348-15 Unitronics Vision and Samba Series (Update A) CISA encourages users and administrators to review the newly released ICS advisories for technical details and mitigations.

Source	Long Form Article
Dark Reading by Robert Lemos (6 – 8 Minutes)	**Apache ERP Zero-Day Underscores Dangers of Incomplete Patches** Unknown groups have launched probes against a zero-day vulnerability identified in Apache's OfBiz enterprise resource planning (ERP) framework — an increasingly popular strategy of analyzing patches for ways to bypass software fixes. The 0-day vulnerability (CVE-2023-51467) in Apache OFBiz, disclosed on Dec. 26, allows an attacker to access sensitive information and remotely execute code against applications using the ERP framework, according to an analysis by cybersecurity firm SonicWall. The Apache Software Foundation had originally released a patch for a related issue, CVE-2023-49070, but the fix failed to protect against other variations of the attack. The incident highlights attackers' strategy of scrutinizing any patches released for high-value vulnerabilities — efforts which often result in finding ways around software fixes, says Douglas McKee, executive director of threat research at SonicWall. "Once someone's done the hard work of saying, 'Oh, a vulnerability exists here,' now a whole bunch of researchers or threat actors can look at that one narrow spot, and you've kind of opened yourself up to a lot more scrutiny," he says. "You've drawn attention to that area of code, and if your patch isn't rock solid or something was missed, it's more likely to be found because you've extra eyes on it." SonicWall researcher Hasib Vhora analyzed the Dec. 5 patch and discovered additional ways to exploit the issue, which the company reported to the Apache Software Foundation on Dec. 14.

Source	Long Form Article
	"We were intrigued by the chosen mitigation when analyzing the patch for CVE-2023-49070 and suspected the real authentication bypass would still be present since the patch simply removed the XML RPC code from the application," Vhora stated in an analysis of the issue. "As a result, we decided to dig into the code to figure out the root cause of the auth-bypass issue." Attacks targeted the Apache OfBiz vulnerability prior to its Dec. 26 disclosure. Source: Sonicwall By Dec. 21, five days before the issue was made public, SonicWall had already identified exploitation attempts for the issue. Apache is not alone in releasing a patch that attackers have managed to bypass. In 2020, six out of the 24 vulnerabilities (25%) attacked using zero-day exploits were variations on previously patched security issues, according to data released by Google's Threat Analysis Group (TAG). By 2022, 17 of the 41 vulnerabilities attacked by zero-day exploits (41%) were variants on previously patched issues, Google stated in an updated analysis. The reasons that companies fail to fully patch an issue are numerous, from not understanding the root cause of the problem to dealing with huge backlogs of software vulnerabilities to prioritizing an immediate patch over a comprehensive fix, says Jared Semrau, a senior manager with Google Mandiant's vulnerability and exploitation group. "There is no simple, single answer as to why this happens," he says. "There are several factors that can contribute to [an incomplete patch], but [SonicWall researchers] are absolutely right — a lot of times companies are just patching the known attack vector." Google expects that the share of zero-day exploits that target incompletely patched vulnerabilities to remain a significant factor. From the attacker perspective, finding vulnerabilities in an application is difficult because researchers and threat actors must look through 100,000s or millions of lines of code. By focusing on promising vulnerabilities that may not have been properly patched, attackers can continue to attack a known weak point rather than start from scratch. In many ways, that's what happened with the Apache OfBiz vulnerability. The original report described two problems: an RCE flaw that required access to the XML-RPC interface (CVE-2023-49070) and an authentication bypass problem that provided untrusted attackers with this access. The Apache Software Foundation believed that removing the XML-RPC endpoint would prevent both issues from being exploited, the ASF security response team said a response to questions from Dark Reading. "Unfortunately, we missed that the same authentication bypass also affected other endpoints, not just the XML-RPC one," the team said. "Once we were made aware, the second patch was issued within hours." The vulnerability, tracked by Apache as OFBIZ-12873, "allows attackers to bypass authentication to achieve a simple Server-Side Request Forgery (SSRF)," Deepak Dixit, a member at the Apache Software Foundation, stated on the Openwall mailing list. He credited SonicWall threat researcher Hasib Vhora and two other researchers — Gao Tian and L0ne1y — with finding the issue. Because OfBiz is a framework, and thus part of the software supply chain, the impact of the vulnerability could be widespread. The popular Atlassian Jira project and issue-tracking software, for example, uses the OfBiz library, but whether the exploit could successfully execute on the platform is still unknown, says Sonicwall's McKee. "It's going to depend on the way each company architects their network, in the way they configure the software," he says. "I would say a typical infrastructure would not have this Internet-facing, that it would require some type of VPN or internal access." In any event, companies should take steps and patch any applications known to use OfBiz to the latest version, the ASF security response team said.

Source	Long Form Article
	"Our recommendation for companies that use Apache OFBiz is to follow security best practices, including only giving access to systems to those users that need it, making sure to regularly update your software, and making sure you are well-equipped to respond when a security advisory is published," they said.