Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 10, 2024

Extracted from multiple sources by PT and OTRB, and ST ISAC analysts for the purpose of supporting ISAC member cybersecurity awareness, protection, and mitigation.

Recipients may share this report only within their own immediate organization. No further dissemination is authorized.

AT-A-GLANCE

Executive News

- 8 U.S. Telcos Compromised, Fbi Advises Americans To Use Encrypted Communications
- Indiana Expands Cyber Analysis to Include Water Facilities
- Encrypted Messaging Service Intercepted, 2.3 Million Messages Read By Law Enforcement
- Cat Deploys First Self-Driving 777 Dump Truck for Aggregates Industry
- Ransomware Costs Manufacturing Sector $17bn in Downtime
- Open Source Supply Chain Faces Security Issues
- Top Challenges Faced by CISOs in Securing Automotive Products in 2025

Emerging Threats & Vulnerabilities

- Cisco Warns of Attacks Exploiting Decade-Old ASA Vulnerability
- Detailing the Attack Surfaces of the WolfBox E40 EV Charger
- 'White FAANG' Data Export Attack: A Gold Mine for PII Threats
- SmokeLoader Malware Exploits MS Office Flaws to Steal Browser Credentials
- Gafgyt Malware Broadens Its Scope in Recent Attacks

Attacks, Breaches, & Leaks

- National Public Data Shuts Down Months After Massive Breach
- U.S. Subsidiaries Of Japanese Water Treatment Company, Green Tea Maker Hit With Ransomware
- Unmasking Termite, the Ransomware Gang Claiming the Blue Yonder Attack
- Medical Device Maker Artivion Scrambling to Restore Systems After Ransomware Attack

EXECUTIVE NEWS

8 U.S. Telcos Compromised, Fbi Advises Americans To Use Encrypted Communications
Help Net Security, 12/5/2024

FBI and Cybersecurity and Infrastructure Security Agency (CISA) officials have advised Americans to use encrypted call and messaging apps to protect their communications from threat actors that have – and will – burrow into the networks and systems of US telecommunication companies. NBC News reported that the advice was given during a conference call with the media on Tuesday, during which the official also shared that the compromise of the networks of multiple US telcos by the China-affiliated Salt Typhoon cyber spies is ongoing, and that they can't predict when the attackers will fully evicted. https://www.helpnetsecurity.com/2024/12/05/us-telcos-compromised-fbi-advises-use-of-encrypted-communications/

Indiana Expands Cyber Analysis to Include Water Facilities
Government Technology, 12/3/2024

The Indiana Office of Technology and the Indiana Department of Environmental Management (IDEM) are expanding their partnership with Purdue University and Indiana University (IU) to safeguard an essential utility for state residents: water. The agencies and universities are broadening the scope of their Cybertrack program, adding utilities that manage water and wastewater services to help address vulnerabilities in these local government systems. Through the partnership, cybersecurity experts and students from Purdue's cyberTAP and IU's Center for Applied Cybersecurity Research will evaluate the digital defenses of water and wastewater facilities https://www.govtech.com/security/indiana-expands-cyber-analysis-to-include-water-facilities

Encrypted Messaging Service Intercepted, 2.3 Million Messages Read By Law Enforcement
Malwarebytes, 12/9/2024

European law enforcement agencies have taken down yet another encrypted messaging service mainly used by criminals. The Matrix encrypted messaging service was an invite-only service which was also marketed under the names Mactrix, Totalsec, X-quantum, or Q-safe. Dutch and French authorities started an investigation when the service was found on the phone of a criminal convicted for the murder of Dutch journalist Peter R. de Vries in 2021. The investigators soon found Matrix was technically more complex than previous platforms such as Sky ECC and EncroChat, which were earlier subjects of law enforcement eavesdropping. https://www.malwarebytes.com/blog/news/2024/12/encrypted-messaging-service-intercepted-2-3-million-messages-read-by-law-enforcement

Cat Deploys First Self-Driving 777 Dump Truck for Aggregates Industry
Equipment World, 12/6/2024

Caterpillar demonstrates its fully autonomous 777 rigid-frame dump truck at Luck Stone's Bull Run plant in Chantilly, Virginia. Caterpillar continues its advancements in autonomous haul trucks, revealing its first deployment of the technology for the aggregates industry. Luck Stone's Bull Run Plant in Chantilly, Virginia, becomes the first to run the self-driving Cat 777 rigid-frame dump truck equipped with MineStar Command, Caterpillar's autonomous system. Luck Stone is the largest family-owned and -operated producer of crushed stone, sand and gravel in the U.S. and has been working with Caterpillar for the past two years to expand the autonomous truck fleet and come up with an economically viable solution for the market. https://www.equipmentworld.com/construction-equipment/heavy-equipment/off-road-trucks/article/15709834/cat-deploys-first-selfdriving-777-dump-truck-for-aggregates

Ransomware Costs Manufacturing Sector $17bn in Downtime
Infosecurity Magazine, 11/27/2024

Ransomware attacks on manufacturing companies have caused an estimated $17bn in downtime since 2018. According to new figures by Comparitech, these incidents have disrupted operations at 858 manufacturers worldwide, with each day of downtime costing an average of $1.9m. This significant financial impact stems from the widespread disruption of ransomware attacks. Beyond halting production, they jeopardize customer orders, damage relationships and lead to prolonged recovery efforts. The data published by Comparitech today highlighted a resurgence in ransomware attacks in 2023, with 194 confirmed cases compared to 109 in 2022. https://www.infosecurity-magazine.com/news/ransomware-manufacturing-dollar17b/

Open Source Supply Chain Faces Security Issues
Beta News, 12/3/2024

The open source software supply chain shows signs of 'AppSec exhaustion,' with organizations showing diminished engagement in security practices and struggling to meet vulnerability management goals, according to a new report. The study from Snyk, based on a survey of 453 professionals across application development and security, shows that open-source security is more important than ever, as hackers have recognized the efficiency of targeting open-source software as a single entry point to multiple orgs. But despite how important these issues have become, organizations have dedicated less tooling and training resources to supply chain vulnerabilities compared to 2023.
https://betanews.com/2024/12/02/open-source-supply-chain-faces-security-issues/

Top Challenges Faced by CISOs in Securing Automotive Products in 2025
Hack Read, 12/1/2024

The modern car offers unmatched convenience, but with great tech comes great responsibility. Trends like software-defined vehicles, autonomous driving, and OTA software updates are redefining what's possible for OEMs and users alike. However, for CISOs, this exciting progress brings a host of new challenges. Protecting passenger safety, navigating evolving regulations, and defending brand trust have become as critical as securing corporate networks. The stakes are higher than ever, making cybersecurity a pivotal part of the journey into the future of mobility. https://cybellum.com/blog/top-challenges-faced-by-cisos-in-securing-automotive-products-in-2025/

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Cisco Warns of Attacks Exploiting Decade-Old ASA Vulnerability -*** The vulnerability is tracked as CVE-2014-2120 and it has been described as a medium-severity cross-site scripting (XSS) vulnerability affecting the WebVPN login page of Cisco Adaptive Security Appliance (ASA) products. https://www.securityweek.com/cisco-warns-of-attacks-exploiting-decade-old-asa-vulnerability/
- ***Detailing the Attack Surfaces of the WolfBox E40 EV Charger*** - The WolfBox E40 is a Level 2 electric vehicle charge station designed for residential home use. Its hardware has a minimal user interface, providing a Bluetooth Low Energy (BLE) interface for configuration and an NFC reader for user authentication. Typical for this class of devices, the appliance employs a mobile application for the owner's installation and regular operation of the equipment. https://www.zerodayinitiative.com/blog/2024/12/2/detailing-the-attack-surfaces-of-the-wolfbox-e40-ev-charger
- ***'White FAANG' Data Export Attack: A Gold Mine for PII Threats –*** Researchers are warning that an otherwise positive European data regulation has introduced massive risks to individuals and the companies they work for. https://www.darkreading.com/cyber-risk/white-faang-data-export-attack-pii-threats
- ***SmokeLoader Malware Exploits MS Office Flaws to Steal Browser Credentials –*** Cybersecurity researchers at Fortinet's FortiGuard Labs have discovered a series of new malware attacks targeting companies in Taiwan. The attacks, which have been linked to the SmokeLoader malware, have impacted industries ranging from manufacturing and healthcare to IT and beyond. https://hackread.com/smokeloader-malware-ms-office-flaws-browser-data/
- ***Gafgyt Malware Broadens Its Scope in Recent Attacks -*** Recently, we've observed the Gafgyt malware (also known as Bashlite or Lizkebab) targeting publicly exposed Docker Remote API servers. Traditionally, this malware has focused on vulnerable IoT devices, but we're now seeing a shift in its behavior as it expands its targets beyond its usual scope. https://www.trendmicro.com/en_us/research/24/l/gafgyt-malware-targeting-docker-remote-api-servers.html

ATTACKS, BREACHES & LEAKS

- ***National Public Data Shuts Down Months After Massive Breach*** **-** National Public Data, the data broker that filed for bankruptcy protection after a breach of its systems exposed 2.9 billion records containing the sensitive and personal data of up to 170 million people, has shut down, leaving behind a two-sentence notice on its website along with a brief recap of the attack and steps those affected by it can take. https://securityboulevard.com/2024/12/national-public-data-shuts-down-months-after-massive-breach/
- ***U.S. Subsidiaries Of Japanese Water Treatment Company, Green Tea Maker Hit With Ransomware*** - The U.S. subsidiary of a Japanese water treatment company said ransomware actors have stolen data from systems and encrypted some servers. https://therecord.media/us-subsidiaries-japanese-water-treatment
- ***Unmasking Termite, the Ransomware Gang Claiming the Blue Yonder Attack*** **-** The November ransomware attack on supplier Blue Yonder that affected large companies like Starbucks, Sainsbury's and Morrisons has been claimed by the Termite ransomware group. https://www.infosecurity-magazine.com/news/termite-ransomware-blue-yonder/
- ***Medical Device Maker Artivion Scrambling to Restore Systems After Ransomware Attack*** - Medical devices company Artivion on Monday disclosed a ransomware attack that knocked some of its systems offline, causing disruption to order and shipping processes. https://www.securityweek.com/medical-device-maker-artivion-scrambling-to-restore-systems-after-ransomware-attack/

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

US CERT/ ICS CERT Alerts and Advisories

1. MOBATIME - https://www.cisa.gov/news-events/ics-advisories/icsa-24-345-01
2. Schneider Electric –
    a. https://www.cisa.gov/news-events/ics-advisories/icsa-24-345-02
    b. https://www.cisa.gov/news-events/ics-advisories/icsa-24-345-03
3. National Instruments LabVIEW - https://www.cisa.gov/news-events/ics-advisories/icsa-24-345-04
4. Horner Automation - https://www.cisa.gov/news-events/ics-advisories/icsa-24-345-05
5. Rockwell Automation Arena - https://www.cisa.gov/news-events/ics-advisories/icsa-24-345-06
6. Ruijie Reyee OS (Update A) - https://www.cisa.gov/news-events/ics-advisories/icsa-24-338-01

SUSE Security Updates

1. nvidia-open-driver-G06-signed - https://www.suse.com/support/update/announcement/2024/suse-ru-20244279-1
2. Linux Kernel - https://www.suse.com/support/update/announcement/2024/suse-su-20244276-1

Fedora Security Advisories

1. Retsnoop - https://lwn.net/Articles/1001569
2. Zabbix - https://lwn.net/Articles/1001575
3. Retsnoop - https://lwn.net/Articles/1001570
4. rust-rustls - https://lwn.net/Articles/1001574
5. python3.12 - https://lwn.net/Articles/1001568
6. python-multipart - https://lwn.net/Articles/1001566
7. python-python-multipart - https://lwn.net/Articles/1001567
8. rust-rbspy - https://lwn.net/Articles/1001571

Check Point Security Advisories

1. Microsoft –
    a. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1114.html
    b. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1147.html

Red Hat Security Advisories

1. java-1.8.0-ibm - https://access.redhat.com/errata/RHSA-2024:10926
2. Red Hat OpenShift Service Mesh Containers for 2.4.13 - https://access.redhat.com/errata/RHSA-2024:10907
3. Red Hat JBoss Enterprise Application Platform 7.4.20 - https://access.redhat.com/errata/RHSA-2024:10928

Ubuntu Security Notices

1. Dogtag PKI - https://ubuntu.com/security/notices/USN-7146-1
2. Expat - https://ubuntu.com/security/notices/USN-7145-1

Oracle Linux Security Update

1. Libsoup –
   a. https://lwn.net/Articles/1001578
   b. https://lwn.net/Articles/1001579
2. Kernel –
   a. https://lwn.net/Articles/1001576
   b. https://lwn.net/Articles/1001577

Other

1. Adobe –
   a. https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html
   b. https://helpx.adobe.com/security/products/acrobat/apsb24-92.html
   c. https://helpx.adobe.com/security/products/media-encoder/apsb24-93.html
   d. https://helpx.adobe.com/security/products/illustrator/apsb24-94.html
   e. https://helpx.adobe.com/security/products/after_effects/apsb24-95.html
   f. https://helpx.adobe.com/security/products/animate/apsb24-96.html
   g. https://helpx.adobe.com/security/products/indesign/apsb24-97.html
   h. https://helpx.adobe.com/security/products/pdfl-sdk1/apsb24-98.html
   i. https://helpx.adobe.com/security/products/connect/apsb24-99.html
   j. https://helpx.adobe.com/security/products/substance3d-sampler/apsb24-100.html
   k. https://helpx.adobe.com/security/products/photoshop/apsb24-101.html
   l. https://helpx.adobe.com/security/products/substance3d-modeler/apsb24-102.html
   m. https://helpx.adobe.com/security/products/bridge/apsb24-103.html

n. https://helpx.adobe.com/security/products/premiere_pro/apsb24-104.html
o. https://helpx.adobe.com/security/products/substance3d_painter/apsb24-105.html
p. https://helpx.adobe.com/security/products/framemaker/apsb24-106.html