Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 8, 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.

Critical Infrastructure Security and Resilience Month

The Transportation Systems Sector-Specific Plan

The Transportation Systems Sector-Specific Plan details how the National Infrastructure Protection Plan risk management framework is implemented within the context of the unique characteristics and risk landscape of the sector. Each Sector Risk Management Agency develops a sector-specific plan through a coordinated effort involving its public and private sector partners. The Postal and Shipping Sector was consolidated within the Transportation Systems Sector in 2013 under Presidential Policy Directive 21. The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.
https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- TSA Announces Proposed Rule That Would Require The Establishment Of Pipeline And Railroad Cyber Risk Management Programs
- Updated Fraud Alert from FMSCA
- Man Arrested In Canada Believed To Be Behind Snowflake Customer Breach
- Business Email Compromise (BEC) Impersonation: The Weapon of Choice of Cybercriminals
- Siemens and Rockwell Tackle Industrial Cybersecurity, but Face Customer Hesitation
- Telematics in the Move to Electric Vehicles
- What's Behind Unchecked CVE Proliferation, And What To Do About It

Emerging Threats & Vulnerabilities

- Mack and International trucks affected by Bendix ECU recall
- New Xiū gǒu Phishing Kit Hits UK, US, Japan, Australia Across Key Sectors
- Air Fryers Are The Latest Surveillance Threat You Didn't Consider
- Critical Auth Bugs Expose Smart Factory Gear to Cyberattack
- Hackers Target Critical Zero-Day Vulnerability In PTZ Cameras

Attacks, Breaches, & Leaks

- Ransomware Attack Hits Sunrise Express by Play Group
- Major Oilfield Supplier Hit by Ransomware Attack
- Cisco Says Devhub Site Leak Won't Enable Future Breaches
- Cyberattack Blamed for Statewide Washington Courts Outage

If you have any questions about this document please contact the ISAC at 866-ST-ISAC1 (866.784.7221) or email st-isac@surfacetransportationisac.org

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

TSA Announces Proposed Rule That Would Require The Establishment Of Pipeline And Railroad Cyber Risk Management Programs
TSA, 11/6/2024

The Transportation Security Administration (TSA) published a Notice of Proposed Rulemaking that proposes to mandate cyber risk management and reporting requirements for certain surface transportation owners and operators. "TSA has collaborated closely with its industry partners to increase the cybersecurity resilience of the nation's critical transportation infrastructure," said TSA Administrator David Pekoske. "The requirements in the proposed rule seek to build on this collaborative effort and further strengthen the cybersecurity posture of surface transportation stakeholders. We look forward to industry and public input on this proposed regulation."
https://www.tsa.gov/news/press/releases/2024/11/06/tsa-announces-proposed-rule-would-require-establishment-pipeline-and

Updated Fraud Alert from FMSCA
FMCSA, 11/6/2024

FMCSA has been alerted to a fake action required notice inviting the recipient to contact **Alan Davis via email at adavis@chp.ca.gov or via phone at 916-784-2547**. The same notice is also asking to provide documentation for a Safety Audit to this link: **https://fmcsa-dot-report.com/LIVIEW/pkg_form_START.prc_saz_entry** . See screenshot below for reference. What You Can Do: Do not click any suspicious links, hover over them to see the real email address or URL of that link. Click ONLY on links you deem trustworthy. Visit the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) for more guidance on online deceiving tactics. Learn more about phishing. https://www.fmcsa.dot.gov/registration/fraud-alerts

Man Arrested In Canada Believed To Be Behind Snowflake Customer Breach
Cyber Scoop, 11/5/2024

Canadian authorities have arrested a person suspected of orchestrating a series of data exfiltration attacks targeting customers of the data storage firm Snowflake. Alexander "Connor" Moucka was taken into custody Oct. 30, based on a provisional arrest warrant, according to Canada's Department of Justice. He is scheduled to appear in court Tuesday. The Canadian Department of Justice confirmed to CyberScoop that the arrest was carried out at the request of the United States. While the specific charges against Moucka remain undisclosed, insiders familiar with the case have identified him as a key figure behind the attacks. https://cyberscoop.com/snowflake-breach-suspected-arrested-connor-moucka-waifu/

Business Email Compromise (BEC) Impersonation: The Weapon of Choice of Cybercriminals
Dark Reading, 10/30/2024

VIPRE Security Group, a global leader and award-winning cybersecurity, privacy, and data protection company, has released its Q3 2024 Email Threat Trends Report, shedding light on the evolving cybersecurity landscape. This comprehensive analysis of real-world data reveals the sophisticated strategies and techniques employed by cybercriminals, with a particular persistent focus on the highly lucrative tactic of business email compromise (BEC). VIPRE processed 1.8 billion emails globally, of which 208 million were malicious. In this third quarter of 2024, cybercriminals intensified their efforts to exploit organisational vulnerabilities through employee deception. BEC scams surged, accounting for 58% of phishing attempts. https://www.darkreading.com/cloud-security/business-email-compromise-bec-impersonation-the-weapon-of-choice-of-cybercriminals

Siemens and Rockwell Tackle Industrial Cybersecurity, but Face Customer Hesitation
Security Week, 11/4/2024

SecurityWeek spoke with representatives of industrial giants Siemens and Rockwell Automation to find out how they help customers address some of the most pressing cybersecurity challenges. Cyberattacks can cause significant disruptions and losses for organizations that rely on ICS or other operational technology, whether they directly target ICS, such as in the case of the recent water sector attacks, or they indirectly impact ICS, such as in the case of ransomware attacks, where impact may spill over from the IT environment. Siemens ProductCERT, which manages security issues related to Siemens products and services, told SecurityWeek that it commonly sees cyberattacks resulting in privacy breaches and a production halt. https://www.securityweek.com/siemens-and-rockwell-tackle-industrial-cybersecurity-but-face-customer-hesitation/

Telematics in the Move to Electric Vehicles
Powertorqu, 11/6/2024

Telematics solutions provider Geotab's '2024 State of Commercial Transportation Report' has provided data insights into how transport businesses are using their telematics in the move to electric vehicles. With electric vehicle importing and production continuing to grow in Australia, the reasons to go to an alternative fuel source keep on growing too. Globally, Geotab reports a 300 per cent rise in the percentage of onboarded commercial vehicles in 2023 compared to 2022. How those electric vehicles are used and what types of jobs they take on will be an important area to observe, Geotab Associate Vice President of Sales (APAC) David Brown believes. https://powertorque.com.au/telematics-in-the-move-to-electric-vehicles/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

What's Behind Unchecked CVE Proliferation, And What To Do About It
Security Intelligence, 11/1/2024

The volume of Common Vulnerabilities and Exposures (CVEs) has reached staggering levels, placing immense pressure on organizations' cyber defenses. According to SecurityScorecard, there were 29,000 vulnerabilities recorded in 2023, and by mid-2024, nearly 27,500 had already been identified. Meanwhile, Coalition's 2024 Cyber Threat Index forecasts that the total number of CVEs for 2024 will hit 34,888—a 25% increase compared to the previous year. This upward trend presents a significant challenge for organizations trying to manage vulnerabilities and mitigate potential exploits. What's behind the dramatic rise in CVEs? And what can security teams do to minimize the risk? Let's find out.
https://securityintelligence.com/articles/whats-behind-unchecked-cve-proliferation-what-to-do/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Mack And International Trucks Affected By Bendix Ecu Recall -*** Bendix's vast equipment recall of hundreds of thousands of electronic control units has affected tens of thousands of Mack trucks and more than 100,000 International trucks. https://landline.media/mack-and-international-trucks-affected-by-bendix-ecu-recall/
- ***New Xiū gǒu Phishing Kit Hits UK, US, Japan, Australia Across Key Sectors –*** Cybersecurity researchers uncovered the "Xiū gǒu" phishing kit targeting users in the UK, US, Spain, Australia, and Japan. Active across public, postal, and banking sectors, the kit mimics legitimate services to harvest data. https://hackread.com/gou-phishing-kit-hits-uk-us-japan-australia-sectors/
- ***Air Fryers Are The Latest Surveillance Threat You Didn't Consider*** - Consumer group Which? has warned shoppers to be selective when it comes to buying smart air fryers from Xiaomi, Cosori, and Aigostar. We've learned to expect that "smart" appliances come with privacy risks—toothbrushes aside—but I really hadn't given my air fryer any thought. Now things are about to change. https://www.malwarebytes.com/blog/news/2024/11/air-fryers-are-the-latest-surveillance-threat-you-didnt-consider
- ***Critical Auth Bugs Expose Smart Factory Gear to Cyberattack*** - Critical security vulnerabilities affecting factory automation software from Mitsubishi Electric and Rockwell Automation could variously allow remote code execution (RCE), authentication bypass, product tampering, or denial-of-service (DoS). https://www.darkreading.com/vulnerabilities-threats/critical-auth-bugs-smart-factory-cyberattack
- ***Hackers Target Critical Zero-Day Vulnerability In PTZ Cameras*** - Hackers are attempting to exploit two zero-day vulnerabilities in PTZOptics pan-tilt-zoom (PTZ) live streaming cameras used in industrial, healthcare, business conferences, government, and courtroom settings. https://www.bleepingcomputer.com/news/security/hackers-target-critical-zero-day-vulnerability-in-ptz-cameras/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Ransomware Attack Hits Sunrise Express by Play Group*** – Sunrise Express Inc., a prominent player in the transportation sector, has recently been targeted by the notorious Play ransomware group. This attack has raised significant concerns about data security and operational integrity within the company. https://ransomwareattacks.halcyon.ai/attacks/ransomware-attack-hits-sunrise-express-by-play-group
- ***Major Oilfield Supplier Hit by Ransomware Attack*** - A ransomware attack has significantly disrupted the operations of a key supplier to the US oil industry. In a regulatory filing sent to the US Securities and Exchange Commission (SEC) on November 7, Texan company Newpark Resources said an unauthorized third party gained access to some of its internal information systems on October 29, an intrusion that led to a ransomware attack. https://www.infosecurity-magazine.com/news/newpark-resources-oilfield/
- ***Cisco Says Devhub Site Leak Won't Enable Future Breaches*** - Cisco says that non-public files recently downloaded by a threat actor from a misconfigured public-facing DevHub portal don't contain information that could be exploited in future breaches of the company's systems. https://www.bleepingcomputer.com/news/security/cisco-says-devhub-site-leak-wont-enable-future-breaches/
- ***Cyberattack Blamed for Statewide Washington Courts Outage*** - The Washington courts network was affected by a cyberattack that led to a statewide outage, the Washington State Administrative Office of the Courts (AOC) announced. https://hackread.com/hackers-claim-access-nokia-internal-data-selling-20k/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. PackageKit - https://www.suse.com/support/update/announcement/2024/suse-ru-20243947-1
2. Qemu - https://www.suse.com/support/update/announcement/2024/suse-su-20243948-1
3. apache2 - https://www.suse.com/support/update/announcement/2024/suse-su-20243949-1
4. govulncheck-vulndb - https://www.suse.com/support/update/announcement/2024/suse-su-20243950-1
5. yast2-bootloader - https://www.suse.com/support/update/announcement/2024/suse-ru-20243951-1
6. libproxy - https://www.suse.com/support/update/announcement/2024/suse-ru-20243952-1
7. firewalld - https://www.suse.com/support/update/announcement/2024/suse-ru-20243953-1
8. java-21-openjdk - https://www.suse.com/support/update/announcement/2024/suse-su-20243954-1
9. python311 –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20243957-1
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20243958-1
10. python312 - https://www.suse.com/support/update/announcement/2024/suse-su-20243959-1
11. libheif - https://www.suse.com/support/update/announcement/2024/suse-su-20243960-1

Fedora Security Advisories

1. thunderbird - https://lwn.net/Articles/997460

Red Hat Security Advisories

1. OpenShift Container Platform 4.14.40 - https://access.redhat.com/errata/RHSA-2024:8700

Ubuntu Security Notices

1. Cinder - https://ubuntu.com/security/notices/USN-6882-2

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ZERO DAY INITIATIVE ADVISORIES & UPDATES

1. Delta –
    a. https://www.zerodayinitiative.com/advisories/ZDI-24-1461/
    b. https://www.zerodayinitiative.com/advisories/ZDI-24-1462/
    c. https://www.zerodayinitiative.com/advisories/ZDI-24-1463/
    d. https://www.zerodayinitiative.com/advisories/ZDI-24-1464/
    e. https://www.zerodayinitiative.com/advisories/ZDI-24-1465/
    f. https://www.zerodayinitiative.com/advisories/ZDI-24-1466/
    g. https://www.zerodayinitiative.com/advisories/ZDI-24-1467/
    h. https://www.zerodayinitiative.com/advisories/ZDI-24-1468/
    i. https://www.zerodayinitiative.com/advisories/ZDI-24-1469/
    j. https://www.zerodayinitiative.com/advisories/ZDI-24-1470/