Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 12, 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

Transportation Systems Sector Cybersecurity Framework Implementation Guide

The Transportation Systems Sector Cybersecurity Framework Implementation Guidance and its companion workbook provide an approach for Transportation Systems Sector owners and operators to apply the tenets of the National Institute of Standards and Technology Cybersecurity Framework to help reduce cyber risks. Specifically, organizations may use the implementation guidance to:

- Characterize their current cybersecurity posture.
- Identify opportunities for enhancing existing cyber risk management programs.
- Find existing tools, standards, and guides to support Framework implementation.
- Communicate their risk management issues to internal and external stakeholders

Organizations that lack a formal cybersecurity risk management program could use the guidance to establish risk-based cyber priorities. https://www.cisa.gov/resources-tools/resources/transportation-systems-sector-cybersecurity-framework-implementation-guide

Additional Resources:

- National Institute of Standards and Technology Cybersecurity Framework http://www.nist.gov/cyberframework/
- Transportation Systems Sector Cybersecurity Framework Implementation Guide https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- Interpol Disrupts Cybercrime Activity On 22,000 IP Addresses, Arrests 41
- Intelligent Rail Summit '24: 'Perfect Forum' For Rail Experts Kicks Off In Estonia
- China's Elite Hackers Expand Target List To European Union
- Mack Has Built More Than 200,000 Telematics-Connected Class 8 Trucks Since 2014
- Third-Party Validation: Table Stakes For Driverless Trucking
- API Security: The Non-Negotiable for Modern Transportation
- The Coming Of 6g Poses New Iot Security Vulnerabilities

Emerging Threats & Vulnerabilities

- Iranian APT Group Targets IP Cameras, Extends Attacks Beyond Israel
- Researcher Discloses 36 Vulnerabilities Found in IBM Security Verify Access
- Fake LockBit, Real Damage: Ransomware Samples Abuse Amazon S3 to Steal Data
- Malware Campaign Uses Ethereum Smart Contracts to Control npm Typosquat Packages
- Android Flaw CVE-2024-43093 May Be Under Limited, Targeted Exploitation

Attacks, Breaches, & Leaks

- Amazon Confirms Employee Data Breach After Vendor Hack
- City Of Sheboygan Dealing With Cyberattack, Ransom Demanded
- New York Press Association Data Breach
- Law Firm Data Breach Impacts 300,000 Presbyterian Healthcare Patients

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

Interpol Disrupts Cybercrime Activity On 22,000 IP Addresses, Arrests 41
Bleeping Computer, 11/5/2024

Interpol announced it arrested 41 individuals and taken down 1,037 servers and infrastructure running on 22,000 IP addresses facilitating cybercrime in an international law enforcement action titled Operation Synergia II. The operation took place between April and August 2024, spanning 95 countries and resulting in 41 arrests of those linked to various crimes, including ransomware, phishing, and information stealers. Interpol said its enforcement action was backed by intelligence provided by private cybersecurity firms like Group-IB, Kaspersky, Trend Micro, and Team Cymru, leading to the identification of over 30,000 suspicious IP addresses. Eventually, roughly 76% of those were taken down, 59 servers were seized, and 43 electronic devices were confiscated, which will be examined to retrieve additional evidence. https://www.bleepingcomputer.com/news/security/interpol-disrupts-cybercrime-activity-on-22-000-ip-addresses-arrests-41/

Intelligent Rail Summit '24: 'Perfect Forum' For Rail Experts Kicks Off In Estonia
Rail Tech, 11/11/2024

Amid the EU's push to expand and standardise rail networks across the continent, the tech that stabilises operations, enhances safety, and optimises efficiency is becoming ever more important. But how do we go about successfully integrating such rapidly advancing tools—AI, big data, and machine learning—on such a massive scale? Well, no one is perhaps better acquainted with this than Emilien Dang, the Chief Technical Officer of RB Rail AS, the joint venture company established by Estonia, Latvia, and Lithuania to coordinate the Rail Baltica project. Managing all technical aspects of one of the most far-reaching rail projects in Europe, he is also one of our esteemed guest speakers at IRS24. Taking a break from overseeing the multi-billion euro programme
https://www.railtech.com/all/2024/11/11/intelligent-rail-summit-24-perfect-forum-for-rail-experts-kicks-off-in-estonia/?gdpr=accept

China's Elite Hackers Expand Target List To European Union
Cyber Scoop, 11/7/2024

China's elite government-backed hackers are using legitimate VPN tools to camouflage their presence on the expanding list of victim networks, according to a new report from the cybersecurity firm ESET. Released Thursday, ESET's report on the latest state-backed cybersecurity threats detail a growing target list that experts believe is a concerted effort to further Beijing's intelligence goals. The Chinese-linked group, referred to as MirrorFace, typically targets the region around Japan, however MirrorFace was recently seen targeting an organization in the European Union. https://cyberscoop.com/china-apt-eset-target-typhoon-mirrorface/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Mack Has Built More Than 200,000 Telematics-Connected Class 8 Trucks Since 2014
Recycling Product News, 11/7/2024

Mack Trucks has achieved a significant milestone in its connected vehicle journey, with more than 200,000 Class 8 trucks built with its proprietary telematics gateway since 2014. Mack says that this achievement underscores its commitment to "maximizing customer uptime through innovative connectivity solutions". Connected Mack trucks are supported around the clock by Mack OneCall agents at the company's Uptime Center, ensuring fleet managers receive continuous support for their operations. "This milestone represents more than just connected trucks — it demonstrates our commitment to providing customers with the tools and support needed to maximize uptime and operational efficiency," says Jonathan Randall, president of Mack Trucks North America.
https://www.recyclingproductnews.com/article/42502/mack-has-built-more-than-200000-telematics-connected-class-8-trucks-since-2014

Third-Party Validation: Table Stakes For Driverless Trucking
Freight Waves, 11/8/2024

In light of Aurora Innovation's decision to push out commercial driverless trucking until next spring, it's worth revisiting how third-party validation is becoming a price of entry for autonomous technology. Much of the public still fears it and would-be users know little about it. Middle-mile autonomous business-to-business logistics leader Gatik and distribution yard autonomy startup Outrider understand their word about safety may not be good enough to earn customer and public trust. AAA's latest survey on autonomous vehicles found U.S. drivers express either fear (66%) or uncertainty (25%) about fully self-driving vehicles. Gatik hired 150-year-old evaluator TÜV SÜD America and software provider Edge Case Research. They reviewed more than 700 safety elements on Isuzu trucks. Some run without safety drivers on short-route routes to and from distribution centers and retail stores.
https://www.freightwaves.com/news/third-party-validation-table-stakes-for-driverless-trucking

API Security: The Non-Negotiable for Modern Transportation
Security Boulevard, 11/5/2024

The transportation sector is undergoing a digital revolution, from railways to aviation and trucking. APIs are at the heart of this transformation, particularly for airlines. Airlines utilize APIs to integrate internal systems with vital services such as booking platforms, check-in services, real-time flight updates, communication with customs agencies, and baggage handling. Ensuring the security of these increasing APIs is critical for protecting passenger data, preventing unauthorized access, and maintaining operational efficiency. As a result, this ensures compliance, fosters passenger trust, and helps avoid service disruptions. The future of safe and reliable transportation relies on robust API security.
https://securityboulevard.com/2024/11/api-security-the-non-negotiable-for-modern-transportation/

The Coming Of 6g Poses New Iot Security Vulnerabilities
Beta News, 11/5/2024

A growing challenge for 6G wireless development involves the potential for unexpected cybersecurity vulnerabilities. This is especially true given the growing set of Internet of Things (IoT) use cases with complexities such as connected cars, smart cities, and even satellite-based (non-terrestrial networks (NTN) IoT. The expanding security threat surface is particularly concerning due to its novelty and the lack of thorough testing by researchers. IoT vulnerabilities themselves are nothing new. We have seen the hacking of home doorbell cameras since the advent of 4G. However, that problem has less to do with wireless standards than with homeowners making poor decisions about how to manage device passwords. https://betanews.com/2024/11/05/the-coming-of-6g-poses-new-iot-security-vulnerabilities/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Iranian APT Group Targets IP Cameras, Extends Attacks Beyond Israel -*** An Iranian cyber-operations group, Emennet Pasargad — also known as Cotton Sandstorm — has broadened its attacks, expanding its targets beyond Israel and the United States and targeting new IT assets, such as IP cameras. https://www.darkreading.com/vulnerabilities-threats/iranian-group-targets-ip-cameras-extends-attacks-beyond-israel
- ***Researcher Discloses 36 Vulnerabilities Found in IBM Security Verify Access –*** Security researcher Pierre Barre has drawn attention to three dozen vulnerabilities in IBM Security Verify Access (ISVA), including ones that could have allowed attackers to compromise the entire authentication infrastructure based on the authorization and network security policy management solution. https://www.securityweek.com/researcher-discloses-32-vulnerabilities-found-in-ibm-security-verify-access/
- ***Fake LockBit, Real Damage: Ransomware Samples Abuse Amazon S3 to Steal Data*** - From infostealer development to data exfiltration, cloud service providers are increasingly being abused by threat actors for malicious schemes. While in this case the ransomware samples we examined contained hard coded AWS credentials, this is specific to this single threat actor and in general, ransomware developers leverage other online services as part of their tactics. https://www.trendmicro.com/en_us/research/24/j/fake-lockbit-real-damage-ransomware-samples-abuse-aws-s3-to-stea.html
- ***Malware Campaign Uses Ethereum Smart Contracts to Control npm Typosquat Packages*** - An ongoing campaign is targeting npm developers with hundreds of typosquat versions of their legitimate counterparts in an attempt to trick them into running cross-platform malware. https://thehackernews.com/2024/11/malware-campaign-uses-ethereum-smart.html
- ***Android Flaw CVE-2024-43093 May Be Under Limited, Targeted Exploitation*** - Google warned that a vulnerability, tracked as CVE-2024-43093, in the Android OS is actively exploited in the wild. https://securityaffairs.com/170581/uncategorized/cve-2024-43093-android-flaw-actively-exploited.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Amazon Confirms Employee Data Breach After Vendor Hack*** – Amazon confirmed a data breach involving employee information after data allegedly stolen during the May 2023 MOVEit attacks was leaked on a hacking forum. https://www.bleepingcomputer.com/news/security/amazon-confirms-employee-data-breach-after-vendor-hack/
- ***City Of Sheboygan Dealing With Cyberattack, Ransom Demanded*** - The city of Sheboygan said a ransom is being demanded after a recent cyberattack. On Nov. 10, the city said an investigation revealed unauthorized access to their network by an external party. Since then, the city has secured its network and is actively working with experts to conduct a thorough forensic review to understand the full scope of the attack. https://www.infosecurity-magazine.com/news/newpark-resources-oilfield/
- ***New York Press Association Data Breach*** - New York Press Association is dedicated to supporting newspapers in enhancing their ability to serve their communities by delivering improved information to their readers. https://www.breachsense.com/breaches/new-york-press-association-data-breach/
- ***Law Firm Data Breach Impacts 300,000 Presbyterian Healthcare Patients*** - In a recent data security incident notice, Thompson Coburn said it had detected unauthorized activity on its network on May 29. An investigation showed that files containing protected health information belonging to patients of its client, Presbyterian Healthcare Services, had been viewed or taken. https://www.securityweek.com/law-firm-data-breach-impacts-300000-presbyterian-healthcare-patients/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

US CERT/ ICS CERT Alerts and Advisories

1. Subnet Solutions - https://www.cisa.gov/news-events/ics-advisories/icsa-24-317-01
2. Hitachi Energy - https://www.cisa.gov/news-events/ics-advisories/icsa-24-317-02
3. Rockwell Automation - https://www.cisa.gov/news-events/ics-advisories/icsa-24-317-03
4. Mitsubishi Electric - https://www.cisa.gov/news-events/ics-advisories/icsa-23-306-03
5. Snap One - https://www.cisa.gov/news-events/alerts/2024/11/12/cisa-releases-five-industrial-control-systems-advisories

SUSE Security Updates

1. python-wxPython - https://www.suse.com/support/update/announcement/2024/suse-su-20243964-1
2. expat - https://www.suse.com/support/update/announcement/2024/suse-su-20243966-1
3. eglexternalplatform - https://www.suse.com/support/update/announcement/2024/suse-ru-20243967-1
4. google-errorprone, guava - https://www.suse.com/support/update/announcement/2024/suse-ru-20241956-2
5. spack - https://www.suse.com/support/update/announcement/2024/suse-ru-20243969-1
6. mojo-parent - https://www.suse.com/support/update/announcement/2024/suse-ru-20243971-1
7. s390-tools - https://www.suse.com/support/update/announcement/2024/suse-ru-20243972-1
8. cosign - https://www.suse.com/support/update/announcement/2024/suse-ru-20243974-1
9. mysql-connector-java - https://www.suse.com/support/update/announcement/2024/suse-ru-20243975-1
10. pcp - https://www.suse.com/support/update/announcement/2024/suse-su-20243976-1
11. xen - https://www.suse.com/support/update/announcement/2024/suse-su-20243977-1

Fedora Security Advisories

1. opendmarc - https://lwn.net/Articles/997723
2. squid –
    a. https://lwn.net/Articles/997729
    b. https://lwn.net/Articles/997730
    c. https://lwn.net/Articles/997731
3. Python-werkzeug - https://lwn.net/Articles/997725
4. Opendmarc - https://lwn.net/Articles/997722
5. xorg-x11-server - https://lwn.net/Articles/997732

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Mageia Security Advisories

1. htmldoc - http://advisories.mageia.org/MGASA-2024-0353.html
2. quictls - http://advisories.mageia.org/MGASA-2024-0354.html
3. python-werkzeug - http://advisories.mageia.org/MGASA-2024-0351.html
4. thunderbird, thunderbird-l10n - http://advisories.mageia.org/MGASA-2024-0350.html

Debian Security Advisories

1. libarchive - https://lists.debian.org/debian-security-announce/2024/msg00220.html
2. nss - https://lists.debian.org/debian-security-announce/2024/msg00221.html
3. ghostscript - https://lists.debian.org/debian-security-announce/2024/msg00222.html
4. symfony - https://lists.debian.org/debian-security-announce/2024/msg00223.html
5. mpg123 - https://lists.debian.org/debian-security-announce/2024/msg00224.html

Slackware Linux Security Advisories

1. wget - http://www.slackware.com/security/viewer.php?l=slackware-security&y=2024&m=slackware-security.343073

Check Point Security Advisories

1. Microsoft –
    a. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-43629
    b. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-43642
    c. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-43630
    d. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-43623

Red Hat Security Advisories

1. python3.12 - https://access.redhat.com/errata/RHSA-2024:9451
2. python3.11-urllib3 - https://access.redhat.com/errata/RHSA-2024:9458
3. buildah - https://access.redhat.com/errata/RHSA-2024:9459
4. osbuild-composer - https://access.redhat.com/errata/RHSA-2024:9456
5. python3.9 - https://access.redhat.com/errata/RHSA-2024:9468
6. grafana-pcp - https://access.redhat.com/errata/RHSA-2024:9472
7. cups - https://access.redhat.com/errata/RHSA-2024:9470
8. Grafana - https://access.redhat.com/errata/RHSA-2024:9473

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Ubuntu Security Notices

1. OpenJDK 21 - https://ubuntu.com/security/notices/USN-7099-1
2. OpenJDK 8 - https://ubuntu.com/security/notices/USN-7096-1
3. OpenJDK 11 - https://ubuntu.com/security/notices/USN-7097-1
4. Linux kernel - https://ubuntu.com/security/notices/USN-7100-1
5. MySQL - https://ubuntu.com/security/notices/USN-7102-1
6. Pydantic - https://ubuntu.com/security/notices/USN-7101-1
7. Ghostscript - https://ubuntu.com/security/notices/USN-7103-1

Zero Day Initiative Advisories & Updates

1. Panda Security Dome - https://www.zerodayinitiative.com/advisories/ZDI-24-1471/

Oracle Linux Security Update

1. Firefox - https://lwn.net/Articles/997742
2. NetworkManager-libreswan –
    a. https://lwn.net/Articles/997743
    b. https://lwn.net/Articles/997744