Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 25, 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

Physical Security

Defending our homeland begins with protecting our nation's hometown security – our physical security. Providing comprehensive physical security requires expertise across a broad range of physical environments and threat types. There are a vast number of physical locations that must be protected. These locations are vulnerable to active shooter, bombing, unmanned aircraft, vehicle ramming as well as insider threat attacks. There are preventative and protective strategies that can be implemented at the federal, state, local, and tribal government levels, within business and organizational structures, and for each individual citizen to safeguard our nation's physical security. For free security and resilience tools and resources, visit: https://www.cisa.gov/topics/physical-security

Additional Resources:

- Active Shooter Preparedness: https://www.cisa.gov/topics/physical-security/active-shooter-preparedness
- Bombing Prevention: https://www.cisa.gov/topics/physical-security/bombing-prevention
- Insider Threat Mitigation: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation
- Vehicle Ramming Mitigation: https://www.cisa.gov/topics/physical-security/vehicle-ramming-mitigation
- Unmanned Aircraft Systems (UAS): https://www.cisa.gov/sites/default/files/publications/uas-ci-challenges-fact-sheet-508.pdf

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- CISA Releases Insights from Red Team Assessment of a U.S. Critical Infrastructure Sector Organization
- U.S. Coast Guard Issues Marsec Directive 105-5 For Chinese-Made Sts Cranes Amid Rising Security Concerns
- Github Projects Targeted With Malicious Commits To Frame Researcher
- Companies Take Over Seven Months to Recover From Cyber Incidents
- Carmen+ UTC Symposium Tackles PNT, Cybersecurity Challenges
- Perspective: Getting Endpoint Security Right
- Combating the Rise of Federally Aimed Malicious Intent

Emerging Threats & Vulnerabilities

- 8.8 Rated PostgreSQL Vulnerability Puts Databases at Risk
- watchTowr Finds New Zero-Day Vulnerability in Fortinet Products
- Researchers Warn of Privilege Escalation Risks in Google's Vertex AI ML Platform
- Botnet Exploits Geovision Zero-Day To Install Mirai Malware
- Palo Alto Networks Releases IoCs for New Firewall Zero-Day

Attacks, Breaches, & Leaks

- HM Environmental Services Data Breach
- Tesla Data Breach Falsely Claimed By Intelbroker, Third-Party Ev Charging Firm Actually Breached
- Grand Forks Public Schools Loses $2.2M to Phishing Scam
- Cyberattack Disrupts Systems of Gambling Giant IGT

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

CISA Releases Insights from Red Team Assessment of a U.S. Critical Infrastructure Sector Organization
CISA, 11/21/2024

Today, CISA released Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a U.S. Critical Infrastructure Sector Organization in coordination with the assessed organization. This cybersecurity advisory details lessons learned and key findings from an assessment, including the Red Team's tactics, techniques, and procedures (TTPs) and associated network defense activity. This advisory provides comprehensive technical details of the Red Team's cyber threat activity, including their attack path to compromise a domain controller and human machine interface (HMI), which serves as a dashboard for operational technology (OT). https://www.cisa.gov/news-events/alerts/2024/11/21/cisa-releases-insights-red-team-assessment-us-critical-infrastructure-sector-organization

U.S. Coast Guard Issues Marsec Directive 105-5 For Chinese-Made Sts Cranes Amid Rising Security Concerns
Industrial Cyber, 11/19/2024

The U.S. Coast Guard, part of the Department of Homeland Security, published Tuesday a notice in the Federal Register, detailing cyber risk management actions for ship-to-shore (STS) cranes made by Chinese companies. The MARSEC Directive 105-5 underscores growing concerns over potential vulnerabilities in critical maritime infrastructure, particularly those involving foreign-manufactured equipment. The directive adds to the requirements set by MARSEC Directive 105-4 and contains security-sensitive information and, therefore, cannot be made available to the general public. The MARSEC Directive 105-5 address the dominance of STS cranes from PRC companies constitute the largest share of the global STS crane market and nearly 80 percent of those at U.S. https://industrialcyber.co/transport/us-coast-guard-issues-marsec-directive-105-5-for-chinese-made-sts-cranes-amid-rising-security-concerns/

Github Projects Targeted With Malicious Commits To Frame Researcher
Bleeping Computer, 11/16/2024

GitHub projects have been targeted with malicious commits and pull requests, in an attempt to inject backdoors into these projects. Most recently, the GitHub repository of Exo Labs, an AI and machine learning startup, was targeted in the attack, which has left many wondering about the attacker's true intentions. On Tuesday, Alex Cheema, co-founder of EXO Labs warned everyone of an "innocent looking" code change submitted to EXO's GitHub repository. The pull request titled "clarify mlx requirement for deepseek models" attempted to modify the models.py Python file in the Exo's code base by adding a sequence of numbers to it: https://www.bleepingcomputer.com/news/security/github-projects-targeted-with-malicious-commits-to-frame-researcher/

Companies Take Over Seven Months to Recover From Cyber Incidents
Infosecurity Magazine, 11/19/2024

IT decision makers (ITDMs) are overly optimistic about how long it would take their organization to recover from a serious cybersecurity incident, according to new data from Fastly. The cloud services provider polled 1800 ITDMs with responsibility for cybersecurity in organizations across the Americas, Europe, APAC and Japan to compile its Global Security Research Report. The study revealed that it takes 7.34 months on average to fully recover from an incident, 25% longer than 5.85 months predicted by respondents. Recovery times are expected to be even longer (8.14 months) for organizations planning to decrease their cybersecurity investment. The gap between perception and reality (34%) is also greater, with these firms actually taking 10.88 months on average to recover. https://www.infosecurity-magazine.com/news/companies-seven-months-recover/

Carmen+ UTC Symposium Tackles PNT, Cybersecurity Challenges
Inside GNSS, 11/19/2024

The growing threat of spoofing and jamming remains a chief concern, with many talks at the symposium focused on how these threats impact highly automated transportation systems (HAVs) and the importance of developing and adopting CPNT technologies. GPS interference isn't a new threat, but until recently, it's mainly been academic and military concerns. Now, it's becoming a civilian concern as well, with aviation impacted more every day. There's a new sense of urgency to combat these threats, with groups like the U.S. Department of Transportation (DOT)'s Center for Automated Vehicle Research with Multimodal AssurEd Navigation (CARMEN+) leading the charge to develop and adopt complementary PNT (CPNT) technologies to strengthen and augment GNSS.
https://insidegnss.com/carmen-utc-symposium-tackles-pnt-cybersecurity-challenges/

Perspective: Getting Endpoint Security Right
Transport Topics, 11/14/2024

Cybercriminals targeting today's supply chain enjoy a smorgasbord of opportunities to crack into companies' data. Every in-cab computer and shipping container sensor serves as a gateway — or, more specifically, a connected "endpoint" — into an increasingly complex device network that keeps the logistics industry moving. While these innovations are designed to drive efficiency, insight and responsiveness, this tech boom is a double-edged sword for companies. In this new landscape, securing logistics endpoints is no longer just an IT concern — it's a critical business imperative that demands the same attention as safeguarding physical cargo. https://www.ttnews.com/articles/endpoint-cybersecurity-logistics

Combating the Rise of Federally Aimed Malicious Intent
Dark Reading, 11/11/2024

Threat actors are exploiting the various ways that zip files combine multiple archives into one file as an anti-detection tactic in phishing attacks that deliver various Trojan malware strains, including SmokeLoader. Attackers are abusing the structural flexibility of zip files through a technique known as concatenation, a method that involves appending multiple zip archives into a single file, new research from Perception Point has found. In this method, the combined file appears as one archive that actually contains multiple central directories, each pointing to different sets of file entries.
https://www.darkreading.com/threat-intelligence/flexible-structure-zip-archives-exploited-hide-malware-undetected

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***8.8 Rated PostgreSQL Vulnerability Puts Databases at Risk*** - Cybersecurity researchers at Varonis have identified a serious security vulnerability in PostgreSQL that could lead to data breaches and system compromise. Learn about the technical details, affected versions, and how to mitigate this threat. https://hackread.com/postgresql-vulnerability-puts-databases-at-risk/
- ***watchTowr Finds New Zero-Day Vulnerability in Fortinet Products*** - Attack surface management provider watchTowr claims to have found a new zero-day vulnerability in cybersecurity provider Fortinet's products. This flaw would allow a managed FortiGate device to elevate privileges and seize control of the FortiManager instance. https://www.infosecurity-magazine.com/news/watchtowr-new-vulnerability/
- ***Researchers Warn of Privilege Escalation Risks in Google's Vertex AI ML Platform –*** Cybersecurity researchers have disclosed two security flaws in Google's Vertex machine learning (ML) platform that, if successfully exploited, could allow malicious actors to escalate privileges and exfiltrate models from the cloud. https://thehackernews.com/2024/11/researchers-warn-of-privilege.html
- ***Botnet Exploits Geovision Zero-Day To Install Mirai Malware –*** A malware botnet is exploiting a zero-day vulnerability in end-of-life GeoVision devices to compromise and recruit them for likely DDoS or cryptomining attacks. https://www.bleepingcomputer.com/news/security/botnet-exploits-geovision-zero-day-to-install-mirai-malware/
- ***Palo Alto Networks Releases IoCs for New Firewall Zero-Day -*** The company recently came across claims regarding a previously unknown remote code execution vulnerability in its PAN-OS operating system. A security advisory published by the company on November 8 urged customers to ensure that access to the PAN-OS management interface is secured, but said there had been no indication of a zero-day being exploited in attacks. https://www.securityweek.com/palo-alto-networks-releases-iocs-for-new-firewall-zero-day/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***HM Environmental Services Data Breach*** **-** HM Environmental Services, Inc. is a full-service environmental remediation contractor licensed to transport hazardous and non-hazardous waste in the Midwest. https://www.breachsense.com/breaches/hm-environmental-services-data-breach/
- ***Tesla Data Breach Falsely Claimed By Intelbroker, Third-Party Ev Charging Firm Actually Breached***- The incident was claimed by CyberN——s members IntelBroker and EnergyWeaponUser, who originally said it was a Tesla EV charging station database containing files that belonged to Tesla. https://databreaches.net/2024/11/22/tesla-data-breach-falsely-claimed-by-intelbroker-third-party-ev-charging-firm-actually-breached/
- ***Grand Forks Public Schools Loses $2.2M to Phishing Scam*** Scammers stole millions from a North Dakota school district by convincing an employee to click on a fraudulent link. The FBI's Internet Crime Report found phishing was by far the most common type of cyber crime last year. https://www.govtech.com/education/k-12/grand-forks-public-schools-loses-2-2m-to-phishing-scam
- ***Cyberattack Disrupts Systems of Gambling Giant IGT*** - Gambling and lottery giant International Game Technology (IGT) has taken certain systems offline after falling victim to a cyberattack over the weekend. https://www.securityweek.com/cyberattack-disrupts-systems-of-gambling-giant-igt/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. nfs-utils - https://www.suse.com/support/update/announcement/2024/suse-ru-20244043-1
2. hwdata - https://www.suse.com/support/update/announcement/2024/suse-ru-20244044-1
3. patterns-base - https://www.suse.com/support/update/announcement/2024/suse-ru-20244045-1
4. rsyslog - https://www.suse.com/support/update/announcement/2024/suse-ru-20244046-1
5. rubygem-yard - https://www.suse.com/support/update/announcement/2024/suse-ru-20244047-1
6. MozillaThunderbird - https://www.suse.com/support/update/announcement/2024/suse-su-20244050-1
7. glib2 - https://www.suse.com/support/update/announcement/2024/suse-su-20244051-1

Fedora Security Advisories

1. needrestart –
    a. https://lwn.net/Articles/999569
    b. https://lwn.net/Articles/999570
    c. https://lwn.net/Articles/999568

Debian Security Advisories

1. Linux - https://lists.debian.org/debian-security-announce/2024/msg00233.html

Check Point Security Advisories

1. Splunk - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0560.html
2. Wordpress Really simple security plugin - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1070.html
3. Microsoft –
    a. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2011-0791.html
    b. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2009-0631.html
4. Palo Alto –
    a. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1075.html
    b. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1076.html
5. Cisco - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2018-2854.html
6. Fortinet - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1073.html
7. VMware - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2019-3175.html

8. Elastic Kibana - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2018-2582.html
9. SonicWall - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2021-2129.html
10. Netgate - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1045.html
11. Qualcomm - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2020-4214.html
12. Polarisoffice - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2018-2722.html

Red Hat Security Advisories

1. Red Hat Data Grid 8.5.2 - https://access.redhat.com/errata/RHSA-2024:10214
2. Red Hat OpenShift Dev Spaces 3.17.0 - https://access.redhat.com/errata/RHSA-2024:10236
3. Pam - https://access.redhat.com/errata/RHSA-2024:10232
4. Red Hat JBoss Enterprise Application Platform 7.3.11 - https://access.redhat.com/errata/RHSA-2024:10207
5. Red Hat JBoss Enterprise Application Platform 7.1.8 - https://access.redhat.com/errata/RHSA-2024:10208
6. perl-App-cpanminus - https://access.redhat.com/errata/RHSA-2024:10218

Ubuntu Security Notices

1. OpenJDK 23 - https://ubuntu.com/security/notices/USN-7124-1
2. Linux kernel - https://ubuntu.com/security/notices/USN-7121-3

TOOL NEWS & UPDATES

Tools & Initiatives

- Faraday 5.9.0 - https://packetstormsecurity.com/files/download/182758/faraday-5.9.0.tar.gz
- Proxmark3 4.19552 Custom Firmware - https://packetstormsecurity.com/files/download/182754/proxmark3-4.19552.tar.gz