Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 7, 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

Moving millions of people and goods across the country daily, the Transportation Systems Sector provides critical lifeline services for communities, supports national defense, and facilitates response and recovery operations. The Sector consists of seven key subsectors or modes: Mass Transit and Passenger Rail, Highway and Motor Carrier, Freight Rail, Maritime Transportation Systems, Pipeline Systems, Aviation, and Postal and Shipping. The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector Risk Management Agencies for the Transportation Systems Sector. This vast network of public and private critical infrastructure owners and operators, the infrastructure and services they manage, and the extensive interdependencies among the transportation modes and other sectors are exposed to myriad of threats and risks, necessitating coordinated planning and investments to manage all hazards efficiently and effectively.

https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructuresectors/transportation-systems-sector

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- Sophos Reveals 5-Year Battle With Chinese Hackers Attacking Network Devices
- Ex-Disney Employee Charged With Hacking Menu Database
- Cisco Patches Critical Vulnerability in Industrial Networking Solution
- New Algorithm Identifies Increase in Critical Infrastructure Security Vulnerabilities
- The Impact of EN 50716:2023 on Rail Digitalization and Advanced Technologies
- Quishing: A Growing Threat Hiding In Plain Sight
- How Carriers Seek To Avoid Multimillion-Dollar Cybersecurity Mistakes

Emerging Threats & Vulnerabilities

- North Korean Hackers Team Up with Play Ransomware in Global Attack
- NVIDIA Shader Out-Of-Bounds And Eleven Levelone Router Vulnerabilities
- Yahoo Discloses NetIQ iManager Flaws Allowing Remote Code Execution
- Qbittorrent Fixes Flaw Exposing Users To MitM Attacks For 14 Years
- LiteSpeed Cache Plugin Vulnerability Poses Admin Access Risk

Attacks, Breaches, & Leaks

- Cyberattack Disables Tracking Systems And Panic Alarms On British Prison Vans
- Fuelco Data Breach
- [LYNX] – Ransomware Victim: plowmancraven[.]co[.]uk
- Hackers Leak 300,000 MIT Technology Review Magazine User Records
- La Housing Authority Confirms Breach Claimed By Cactus Ransomware

SENSITIVE & PROPRIETARY INFROMATION - NOT FOR PUBLIC DISSEMINATION

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

EXECUTIVE NEWS

Sophos Reveals 5-Year Battle With Chinese Hackers Attacking Network Devices
Bleeping Computer, 10/31/2024

Sophos disclosed today a series of reports dubbed "Pacific Rim" that detail how the cybersecurity company has been sparring with Chinese threat actors for over 5 years as they increasingly targeted networking devices worldwide, including those from Sophos. For years, cybersecurity firms have warned enterprises that Chinese threat actors exploit flaws in edge networking devices to install custom malware that allows them to monitor network communications, steal credentials, or act as proxy servers for relayed attacks. These attacks have targeted well-known manufacturers, including Fortinet, Barracuda, SonicWall, Check Point, D-Link, Cisco, Juniper, NetGear, Sophos, and many more. https://www.bleepingcomputer.com/news/security/sophos-reveals-5-year-battle-with-chinese-hackers-attacking-network-devices/

Ex-Disney Employee Charged With Hacking Menu Database
Dark Reading, 10/30/2024

A former Disney employee was arrested and charged after allegedly hacking into the company's systems and altering its restaurant menus. Michael Scheuer, an ex-menu production manager at Disney, was charged with violating the Computer Fraud and Abuse Act (CFAA) on three different occasions. He was fired from this position in June, after unspecified misconduct; his dismissal was described as "contentious" and "not considered to be amicable," according to court documents. Scheuer allegedly used his work credentials, which were still functioning after his termination, to log into the Disney menu creation system contracted by a third-party company and change the fonts in the system to Wingdings symbols. https://www.darkreading.com/cyberattacks-data-breaches/ex-disney-employee-charged-hacking-menu-database

Cisco Patches Critical Vulnerability in Industrial Networking Solution
Security Week, 11/7/2024

The critical bug, tracked as CVE-2024-20418 (CVSS score of 10/10), allows a remote, unauthenticated attacker to inject commands on the underlying operating system, with root privileges. The issue exists because the web-based management interface of the industrial networking solution does not properly validate input, allowing an attacker to send crafted HTTP requests. “A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system of the affected device,” Cisco notes in its advisory. The security defect affects the company’s Catalyst IW9165D, IW9165E, and IW9167E access points that have the Ultra-Reliable Wireless Backhaul (URWB) operating mode enabled. https://www.securityweek.com/cisco-patches-critical-vulnerability-in-industrial-networking-solution/

New Algorithm Identifies Increase in Critical Infrastructure Security Vulnerabilities
Georgia Tech, 10/11/2024

Behind the normalcy of daily life is critical infrastructure. It's responsible for keeping water clean, providing electricity, and facilitating the supply chain ensuring the needs of countless people around the world are met. As with most systems, the technology that helps operate, manage, and monitor critical infrastructure can be connected to the internet, making it vulnerable to cyberattacks. Just last year, a water treatment plant in Pennsylvania was attacked by Iranian hackers and taken offline. Russia is also currently using cyberattacks to interfere with the Ukrainian power grid. These attacks are becoming more frequent and more powerful, with the capability to shut down large operations, adversely affecting millions of people. https://ece.gatech.edu/news/2024/10/new-algorithm-identifies-increase-critical-infrastructure-security-vulnerabilities-0

The Impact of EN 50716:2023 on Rail Digitalization and Advanced Technologies
Embedded, 11/6/2024

The digitalization of the rail industry has and continues to revolutionize how rail systems are designed, operated, and maintained. Advanced digital technologies have been integrated into most aspects of rail operations to enhance efficiency, safety, and passenger experiences. Sensors and Internet of Things (IoT) devices are being deployed extensively across rail networks to monitor track conditions, train performance, and environmental factors in real time. This data drives predictive maintenance, reducing downtime and improving safety. Additionally, rail operators utilize big data analytics to process vast amounts of data collected from various sources to optimize schedules, improve resource allocation, and enhance decision-making processes. https://www.embedded.com/the-impact-of-en-507162023-on-rail-digitalization-and-advanced-technologies

Quishing: A Growing Threat Hiding In Plain Sight
Security Intelligence, 10/31/2024

Our mobile devices go everywhere we go, and we can use them for almost anything. For businesses, the accessibility of mobile devices has also made it easier to create more interactive ways to introduce new products and services while improving user experiences across different industries. Quick-response (QR) codes are a good example of this in action and help mobile devices quickly navigate to web pages or install new software by simply scanning an image. However, legitimate organizations aren’t the only ones generating QR codes for added convenience. Cyber criminals are also leveraging QR codes and the increased reliance on near-field technology (NFC) to launch sophisticated attacks on unsuspecting victims. https://securityintelligence.com/articles/quishing-growing-threat-hiding-plain-sight/

How Carriers Seek To Avoid Multimillion-Dollar Cybersecurity Mistakes
Trucking Dive, 11/4/2024

When Werner Enterprises workers saw a video of CEO Derek Leathers apparently announcing an end to all employee vacations, responses ranged from “this is crazy” to “I’m leaving.” But the company created the ruse using a software tool and previous footage of Leathers. Werner was prompted by growing concerns a year and a half ago that a real cyberattack could mislead workers. The company informed staff at an all-hands meeting 90 minutes after the broadcast occurred that it was fake, EVP and CIO Daragh Mahon said last week at the National Motor Freight Traffic Association Cybersecurity Conference in Cleveland. https://www.truckingdive.com/news/nmfta-2024-cybersecurity-conference-ransomware-deep-fake-email-phishing/731753/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202024-11-04%20Trucking%20Dive%20%5Bissue:67490%5D&utm_term=Trucking%20Dive

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***North Korean Hackers Team Up with Play Ransomware in Global Attack -*** North Korean state-sponsored threat group, Jumpy Pisces, collaborated with the Play ransomware group to carry out cyberattacks. Learn about the tools and techniques used, the impact of the attack, and how to protect your organization from similar threats. https://hackread.com/north-korean-hackers-play-ransomware-global-attack/
- ***NVIDIA Shader Out-Of-Bounds And Eleven Levelone Router Vulnerabilities –*** Cisco Talos' Vulnerability Research team recently discovered five Nvidia out-of-bounds access vulnerabilities in shader processing, as well as eleven LevelOne router vulnerabilities spanning a range of possible exploits. https://blog.talosintelligence.com/nvidia-shader-out-of-bounds-and-level1-2/
- ***Yahoo Discloses NetIQ iManager Flaws Allowing Remote Code Execution*** - Yahoo's Paranoid vulnerability research team has identified nearly a dozen flaws in OpenText's NetIQ iManager product, including some that could have been chained for unauthenticated remote code execution. https://www.securityweek.com/yahoo-discloses-netiq-imanager-flaws-allowing-remote-code-execution/
- ***Qbittorrent Fixes Flaw Exposing Users To MitM Attacks For 14 Years*** - qBittorrent has addressed a remote code execution flaw caused by the failure to validate SSL/TLS certificates in the application's DownloadManager, a component that manages downloads throughout the app. https://www.bleepingcomputer.com/news/security/qbittorrent-fixes-flaw-exposing-users-to-mitm-attacks-for-14-years/
- ***LiteSpeed Cache Plugin Vulnerability Poses Admin Access Risk*** - A vulnerability in the LiteSpeed Cache plugin for WordPress, which has over 6 million active installations, has been discovered allowing unauthenticated visitors to gain administrator-level access by exploiting a security flaw in the plugin's role simulation feature. This flaw permitted unauthorized access that could lead to the installation of malicious plugins. https://www.infosecurity-magazine.com/news/litespeed-cache-plugin-flaw-admin/

ATTACKS, BREACHES & LEAKS

- ***Cyberattack Disables Tracking Systems And Panic Alarms On British Prison Vans*** – A cyberattack on a telematics company has left British prison vans without tracking systems or panic alarms, although there is no evidence criminals have attempted to exploit the situation. https://therecord.media/british-prison-vans-cyberattack
- ***Fuelco Data Breach*** - Fuelco has been providing complete fuel storage solutions since 1994. https://www.breachsense.com/breaches/fuelco-data-breach/
- ***[LYNX] – Ransomware Victim: plowmancraven[.]co[.]uk*** - The leak page associated with the construction sector company identified as Plowman Craven presents vital information on their operations. Plowman Craven specializes in integrated measurement and consultancy services for property and infrastructure markets globally, transcending the traditional role of a survey company. https://www.redpacketsecurity.com/lynx-ransomware-victim-plowmancraven-co-uk/
- ***Hackers Leak 300,000 MIT Technology Review Magazine User Records*** - Hackers claim to have breached MIT Technology Review Magazine via a third-party contractor, leaking nearly 300,000 user records on Breach Forums. Data includes full names, email addresses, and activity details, posing risks for phishing and targeted scams. https://hackread.com/hackers-leak-mit-technology-review-user-records/
- ***La Housing Authority Confirms Breach Claimed By Cactus Ransomware*** **-** The Housing Authority of the City of Los Angeles (HACLA), one of the largest public housing authorities in the United States, confirmed that a cyberattack hit its IT network after recent breach claims from the Cactus ransomware gang. https://www.bleepingcomputer.com/news/security/lottiefiles-hacked-in-supply-chain-attack-to-steal-users-crypto/

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

US CERT/ ICS CERT ALERTS AND ADVISORIES

1. Android Framework - https://www.cve.org/CVERecord?id=CVE-2024-43093
2. CyberPanel Incorrect - https://www.cve.org/CVERecord?id=CVE-2024-51567
3. Nostromo nhttpd - https://www.cve.org/CVERecord?id=CVE-2019-16278
4. Palo Alto - https://www.cve.org/CVERecord?id=CVE-2024-5910
5. Beckhoff Automation - https://www.cisa.gov/news-events/ics-advisories/icsa-24-312-01
6. Delta Electronics - https://www.cisa.gov/news-events/ics-advisories/icsa-24-312-02
7. Bosch Rexroth - https://www.cisa.gov/news-events/ics-advisories/icsa-24-312-03

SUSE SECURITY UPDATES

1. Wicked –
   a. https://www.suse.com/support/update/announcement/2024/suse-ru-20243936-1
   b. https://www.suse.com/support/update/announcement/2024/suse-ru-20243935-1
   c. https://www.suse.com/support/update/announcement/2024/suse-ru-20243933-1
   d. https://www.suse.com/support/update/announcement/2024/suse-ru-20243931-1
2. go1.23-openssl - https://www.suse.com/support/update/announcement/2024/suse-su-20243937-1
3. go1.22-openssl - https://www.suse.com/support/update/announcement/2024/suse-su-20243938-1
4. ruby2.1 - https://www.suse.com/support/update/announcement/2024/suse-su-20243939-1
5. ghostscript –
   a. https://www.suse.com/support/update/announcement/2024/suse-su-20243941-1
   b. https://www.suse.com/support/update/announcement/2024/suse-su-20243942-1
6. python3 - https://www.suse.com/support/update/announcement/2024/suse-su-20243944-1

FEDORA SECURITY ADVISORIES

1. firefox - https://lwn.net/Articles/997357

CHECK POINT SECURITY ADVISORIES

1. Apache –
   a. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0663.html
   b. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0407.html

Red Hat Security Advisories

1. Thunderbird –
   a. https://access.redhat.com/errata/RHSA-2024:9015
   b. https://access.redhat.com/errata/RHSA-2024:9017

***** FAIR USE NOTICE*****

This message contains copyrighted material whose use has not been specifically authorized by the copyright owner. The ST-ISAC is making it available to ISAC members who have expressed a prior interest in receiving information to advance their understanding of threat activities in the interest of protecting the national infrastructure of the United States. We believe that this constitutes a 'fair use' of the copyrighted material as provided for in section 107 of the U.S. Copyright Law. If you wish to use this copyrighted material for purposes of your own that go beyond 'fair use,' you must obtain permission from the copyright owner.