Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 6, 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

Vigilance – the Power of Hello

Organizations face a variety of threats, both internal and external, from hostile governments, terrorist groups, disgruntled employees and malicious introducers. Alert employees can spot suspicious activity and report it. The power is in the employee, citizen, patron, or any person who can observe and report. Used effectively, the right words can be a powerful tool. Simply saying "Hello" can prompt a casual conversation with unknown individuals and help you determine why they are there. The OHNO approach – Observe, initiate a Hello, Navigate the Risk, and Obtain Help – helps employees observe and evaluate suspicious behaviors, and empowers them to mitigate potential risk, and obtain help when necessary. The Power of Hello Slick-sheet and Power of Hello Placemat provides stakeholders with information to assist in identifying and effectively responding to suspicious behavior.
https://www.cisa.gov/power-hello

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- Schmitz Cargobull First Manufacturer To Factory-Fit Webfleet Telematics To Its Trailers
- Warning: Hackers Could Take Over Your Email Account By Stealing Cookies, Even If You Have Mfa
- Over Half of U.S. County Websites "Could Be Spoofed"
- Lumma/Amadey: Fake Captchas Want To Know If You're Human
- ChatGPT Can Be Manipulated Using Hex Code
- Sneak Peak: 2025 Cybersecurity Issues In Trucking
- API Security Matters: The Risks of Turning a Blind Eye

Emerging Threats & Vulnerabilities

- Attacker Abuses Victim Resources to Reap Rewards from Titan Network
- 'CrossBarking' Attack Targeted Secret APIs, Exposing Opera Browser Users
- Ransomware Hits Web Hosting Servers Via Vulnerable Cyberpanel Instances
- Chenlun's Evolving Phishing Tactics Target Trusted Brands
- New Research Reveals Spectre Vulnerability Persists in Latest AMD and Intel Processors

Attacks, Breaches, & Leaks

- Canadian Government Data Stolen By Chinese Hackers
- Schneider Electric Reports Cyberattack, Its Third Incident In 18 Months
- L&B Transport Data Breach
- Hackers Claim Access to Nokia Internal Data, Selling for $20,000
- Lottiefiles Hacked In Supply Chain Attack To Steal Users' Crypto

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

Schmitz Cargobull First Manufacturer To Factory-Fit Webfleet Telematics To Its Trailers
MotorTransport, 11/5/2024

Commercial fleet operators can now connect Schmitz Cargobull trailers with Webfleet via factory fitted telematics, eliminating the need for aftermarket hardware installations. This development gives operators access to trailer data to boost trailer utilisation, reduce downtime and improve overall safety and security. Webfleet, which is Bridgestone's fleet management solutions provider, said it has plans to extend the programme to other trailer manufacturers in the future. Taco van der Leij, vice president of Webfleet Europe at Bridgestone Mobility Solutions, said: "Trailers are the backbone of long-haul goods transportation, but managing a trailer fleet can be challenging. https://motortransport.co.uk/industry-news/schmitz-cargobull-first-manufacturer-to-factory-fit-webfleet-telematics-to-its-trailers/24835.article

Warning: Hackers Could Take Over Your Email Account By Stealing Cookies, Even If You Have Mfa
Malwarebytes Labs, 11/5/2024

The Federal Bureau of Investigation (FBI) has issued a warning that cybercriminals are taking over email accounts via stolen session cookies, allowing them to bypass the multi-factor authentication (MFA) a user has set up. Here's how it works. Most of us don't think twice about checking the "Remember me" box when we log in. When you log in and the server has verified your authentication—straight away or after using MFA–the server creates a session and generates a unique session ID. This session ID is stored in a session cookie (or a "Remember-Me cookie" as the FBI calls it) on your browser, which is typically valid for 30 days. Every time you return to that website within the time frame, you don't need to log in. That's really convenient… unless someone manages to steal that cookie from your system. https://www.malwarebytes.com/blog/news/2024/11/warning-hackers-could-take-over-your-email-account-by-stealing-cookies-even-if-you-have-mfa

Over Half of U.S. County Websites "Could Be Spoofed"
Infosecurity Magazine, 10/30/2024

Security experts have sounded another US election warning after claiming that the majority of US county websites could be copied to spread disinformation and steal info. Comparitech analyzed the websites and official contact email addresses for 3144 US counties to compile its report. These administrative districts play an important role in elections, as many voters turn to their local county website for information on polling booths and other queries. However, Comparitech found that 57% of such sites are registered with non-.gov domains, meaning they could easily be spoofed with malign intent. https://www.infosecurity-magazine.com/news/half-us-county-websites-could-be/

Lumma/Amadey: Fake Captchas Want To Know If You're Human
SecureList, 10/29/2024

Attackers are increasingly distributing malware through a rather unusual method: a fake CAPTCHA as the initial infection vector. Researchers from various companies reported this campaign in August and September. The attackers, primarily targeting gamers, initially delivered the Lumma stealer to victims through websites hosting cracked games. Our recent research into the adware landscape revealed that this malicious CAPTCHA is spreading through a variety of online resources that have nothing to do with games: adult sites, file-sharing services, betting platforms, anime resources, and web apps monetizing through traffic. This indicates an expansion of the distribution network to reach a broader victim pool. Moreover, we discovered that the CAPTCHA delivers not only Lumma but also the Amadey Trojan. https://securelist.com/fake-captcha-delivers-lumma-amadey/114312/

ChatGPT Can Be Manipulated Using Hex Code
Dark Reading, 10/28/2024

A new prompt-injection technique could allow anyone to bypass the safety guardrails in OpenAI's most advanced language learning model (LLM). GPT-4o, released May 13, is faster, more efficient, and more multifunctional than any of the previous models underpinning ChatGPT. It can process multiple different forms of input data in dozens of languages, then spit out a response in milliseconds. It can engage in real-time conversations, analyze live camera feeds, and maintain an understanding of context over extended conversations with users. When it comes to user-generated content management, however, GPT-4o is in some ways still archaic. https://www.darkreading.com/application-security/chatgpt-manipulated-hex-code

Sneak Peak: 2025 Cybersecurity Issues In Trucking
Commerical Carrier Journal, 11/1/2024

The cybersecurity team at the National Motor Freight Traffic Association, Inc. (NMFTA) is wasting no time looking ahead to 2025, gearing up to tackle the biggest threats facing the trucking industry in our increasingly digital world, and identifying the most effective solutions to stay ahead of the curve. Currently, the team is crafting bold predictions and recommended strategies for the year ahead, much of which we covered extensively during our sold-out, three-day Cybersecurity Conference in Cleveland, Ohio. If you missed the conference, you missed a remarkable gathering of top cybersecurity and trucking experts. Attendees left with invaluable insights that are set to transform the industry's approach to cyber threats, highlighting the critical intersection of technology and freight security. https://www.ccjdigital.com/technology/cybersecurity/article/15707306/trucking-industry-cybersecurity-2025-nmfta-reveals-emerging-threats

API Security Matters: The Risks of Turning a Blind Eye
Security Week, 10/31/2024

I have the good fortune of traveling a fair bit to meet security teams within businesses that span different sizes, industry verticals, and geographies. During these travels, without fail, I find myself having fascinating conversations that are very grounding and informative regarding the issues and challenges that these security teams are grappling with. As you might expect, these issues and challenges evolve over time as certain ones are addressed and move lower in priority and other ones emerge and become top of mind. Not surprisingly, one topic that has come up repeatedly in the recent past is API Security. To be explicit (and hopefully clear), by API Security, I mean the full lifecycle of API Security. https://www.securityweek.com/api-security-matters-the-risks-of-turning-a-blind-eye/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Attacker Abuses Victim Resources to Reap Rewards from Titan Network -*** Recently, we observed an attack where an attacker exploited the Atlassian Confluence server vulnerability CVE-2023-22527. This allowed unauthenticated attackers to achieve remote code execution (RCE) and leverage the Titan Network for cryptomining activity. https://www.trendmicro.com/en_us/research/24/j/titan-network.html
- ***'CrossBarking' Attack Targeted Secret APIs, Exposing Opera Browser Users –*** Using a malicious Chrome extension, researchers showed how an attacker could use a now-fixed bug to inject custom code into a victim's Opera browser to exploit special and powerful APIs, used by developers and typically saved for only the most trusted sites. https://www.darkreading.com/vulnerabilities-threats/crossbarking-attack-secret-apis-expose-opera-browser-users
- ***Ransomware Hits Web Hosting Servers Via Vulnerable Cyberpanel Instances*** - A threat actor – or possibly several – has hit approximately 22,000 vulnerable instances of CyberPanel and encrypted files on the servers running it with the PSAUX and other ransomware. https://www.helpnetsecurity.com/2024/10/30/vulnerable-cyberpanel-psaux-ransomware/
- ***Chenlun's Evolving Phishing Tactics Target Trusted Brands*** - An ongoing, sophisticated phishing campaign has been observed targeting individuals with text messages impersonating trusted brands like Amazon. DomainTools researchers linked this activity to the threat actor Chenlun, who last year was known for exploiting USPS delivery alerts during the holiday season to lure recipients into providing sensitive information. https://www.infosecurity-magazine.com/news/chenluns-phishing-tactics-target/
- ***New Research Reveals Spectre Vulnerability Persists in Latest AMD and Intel Processors*** -More than six years after the Spectre security flaw impacting modern CPU processors came to light, new research has found that the latest AMD and Intel processors are still susceptible to speculative execution attacks. https://thehackernews.com/2024/10/new-research-reveals-spectre.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Canadian Government Data Stolen By Chinese Hackers*** – At least 20 Canadian government networks have been compromised by Chinese state-sponsored threat actors, who have maintained access over the past four years to steal valuable data. https://www.infosecurity-magazine.com/news/canadian-government-data-chinese/
- ***Schneider Electric Reports Cyberattack, Its Third Incident In 18 Months*** - Multinational energy management company Schneider Electric said Tuesday it was the victim of a cyberattack, with attackers behind a new ransomware variant claiming responsibility. https://cyberscoop.com/schneider-electric-energy-ransomware-hellcat/
- ***L&B Transport Data Breach*** - L&B Transport LLC is a transportation company based in Louisiana, USA. https://www.breachsense.com/breaches/l-b-transport-data-breach/
- ***Hackers Claim Access to Nokia Internal Data, Selling for $20,000*** - Hackers claim to have breached Nokia through a third-party contractor, allegedly stealing SSH keys, source code, and internal credentials. The data is being sold for $20,000 on BreachForums, though no customer data was affected. Nokia has not yet commented on the claim. https://hackread.com/hackers-claim-access-nokia-internal-data-selling-20k/
- ***Lottiefiles Hacked In Supply Chain Attack To Steal Users' Crypto*** - The popular LottieFiles Lotti-Player project was compromised in a supply chain attack to inject a crypto drainer into websites that steals visitors' cryptocurrency. https://www.bleepingcomputer.com/news/security/lottiefiles-hacked-in-supply-chain-attack-to-steal-users-crypto/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. Pipewire - https://www.suse.com/support/update/announcement/2024/suse-ru-20243919-1
2. Libgsf –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20243920-1
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20243921-1
    c. https://www.suse.com/support/update/announcement/2024/suse-su-20243922-1
3. Gradle - https://www.suse.com/support/update/announcement/2024/suse-su-20243923-1
4. Python310 - https://www.suse.com/support/update/announcement/2024/suse-su-20243924-1
5. Curl –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20243925-1
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20243926-1
    c. https://www.suse.com/support/update/announcement/2024/suse-su-20243927-1
6. cloud-regionsrv-client - https://www.suse.com/support/update/announcement/2024/suse-ru-20243928-1
7. python36 - https://www.suse.com/support/update/announcement/2024/suse-su-20243929-1

Gentoo Security Advisories

1. Neat VNC - https://security.gentoo.org/glsa/202411-01
2. Flatpak - https://security.gentoo.org/glsa/202411-02
3. Ubiquiti UniFi - https://security.gentoo.org/glsa/202411-03
4. EditorConfig core C library - https://security.gentoo.org/glsa/202411-04
5. libgit2 - https://security.gentoo.org/glsa/202411-05

Fedora Security Advisories

1. syncthing –
    a. https://lwn.net/Articles/997145
    b. https://lwn.net/Articles/997147
2. php-tcpdf –
    a. https://lwn.net/Articles/997144
    b. https://lwn.net/Articles/997142
3. Thunderbird –
    a. https://lwn.net/Articles/997148
    b. https://lwn.net/Articles/997149

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Debian Security Advisories

1. Thunderbird - https://lists.debian.org/debian-security-announce/2024/msg00217.html

Check Point Security Advisories

1. Wordpress –
    a. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1027.html
    b. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1024.html
2. Netgear –
    a. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1009.html
    b. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1008.html
    c. https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1005.html

Drupal Security Advisories

1. Tooltip - https://www.drupal.org/sa-contrib-2024-058
2. Baisc HTTP Authentication - https://www.drupal.org/sa-contrib-2024-057

Cisco Advisories and Alerts

1. Cisco Unified Industrial Wireless Software - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-backhaul-ap-cmdinj-R7E28Ecs
2. Cisco Nexus Dashboard Fabric Controller SQL - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-sqli-CyPPAxrL
3. Cisco Enterprise Chat and Email Denial of Service Vulnerability - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-dos-Oqb9uFEv
4. Cisco 7800, 8800, and 9800 Series Phones Information Disclosure Vulnerability - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-infodisc-sbyqQVbG
5. Cisco 6800, 7800, 8800, and 9800 Series Phones - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mpp-xss-8tAV2TvF

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Red Hat Security Advisories

1. mod_jk –
    a. https://access.redhat.com/errata/RHSA-2024:8928
    b. https://access.redhat.com/errata/RHSA-2024:8929
2. edk2 - https://access.redhat.com/errata/RHSA-2024:8935
3. OpenShift Container Platform 4.13.53 bug - https://access.redhat.com/errata/RHSA-2024:8688
4. Red Hat Advanced Cluster Management 2.12.0 - https://access.redhat.com/errata/RHSA-2024:8974

Ubuntu Security Notices

1. Linux kernel - https://ubuntu.com/security/notices/USN-7088-3

Oracle Linux Security Update

1. python3.11-urllib3 – https://lwn.net/Articles/997164
2. kernel –
    a. https://lwn.net/Articles/997159
    b. https://lwn.net/Articles/997160
3. Bcc –
    a. https://lwn.net/Articles/997154
4. python-gevent - https://lwn.net/Articles/997163
5. haproxy - https://lwn.net/Articles/997157
6. xmlrpc-c - https://lwn.net/Articles/997166
7. python3.11-urllib3 - https://lwn.net/Articles/997164
8. bpftrace - https://lwn.net/Articles/997155
9. grafana-pcp - https://lwn.net/Articles/997156