Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 4, 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

Help Drive Down Critical Infrastructure Risk and Build Resilience

There are 16 critical infrastructure sectors whose assets, systems, and networks—both physical and virtual— are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or a combination of any of these. Critical infrastructure is a shared resource as well as a shared responsibility. It is important that all individuals and organizations understand the risks; plan, prepare, and train for potential events; and remain vigilant for and report suspicious activity.

https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- Cisa Sees Elimination Of ‘bad Practices’ As Next Secure-By-Design Step
- National Cyber Threat Assessment 2025-2026
- Redline, Meta Infostealer Malware Operations Seized By Police
- How To Build A Next-Generation Of Railway Cybersecurity
- 1,000+ Web Shops Infected By “Phish ‘n Ships” Criminals Who Create Fake Product Listings For In-Demand Products
- Autonomous Discovery of Critical Zero-Days
- Supply Chain Security Is National Security: Cyber, Physical, and Personnel Protections

Emerging Threats & Vulnerabilities

- Cybercriminals Use Webflow to Deceive Users into Sharing Sensitive Login Credentials
- Russian Malware Campaign Targets Ukrainian Recruits Via Telegram
- Fog and Akira ransomware attacks exploit SonicWall VPN flaw CVE-2024-40766
- Black Basta Operators Phish Employees Via Microsoft Teams
- Windows 'Downdate' Attack Reverts Patched PCs to a Vulnerable State

Attacks, Breaches, & Leaks

- Cyber Attack Wipes Out Dhl Delivery Tracking Systems Causing Issues For Nisa Retailers
- Tens Of Thousands Of Taxpayer Accounts Hacked As CRA Repeatedly Paid Out Millions In Bogus Refunds
- California Court Suffering From Tech Outages After Cyberattack
- Italian Politicians Express Alarm at Latest Data Breach Allegedly Affecting 800,000 Citizens

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 Sees Elimination Of 'bad Practices' As Next Secure-By-Design Step
Cyber Scoop, 10/28/2024

A year-and-a-half after launching its global secure-by-design initiative, the Cybersecurity and Infrastructure Security Agency is "thrilled" by the progress it's made in getting vendors on board and now turning its focus to a new program aimed at drawing more attention to especially risky software-building practices. Rina Rakipi, who leads strategic partnerships and vulnerability program development at CISA, said Monday during ACT-IAC's Imagine Nation ELC 2024 conference that the cyber agency has secured more than 230 voluntary commitments from software manufacturers under the campaign. igning on to the secure-by-design initiative means that those vendors pledge to meet within a year a variety of cybersecurity goals https://cyberscoop.com/cisa-secure-by-design-software-bad-practices/

National Cyber Threat Assessment 2025-2026
Canadian Centre for Cyber Security, 11/1/2024

CSE uses its expertise to help monitor, detect, and investigate threats against Canada's information systems and networks. Based on our observations since NCTA 2023-2024, we have identified five trends that will shape Canada's cyber threat environment until 2026: Before discussing the five trends above in more detail, it is important to note that trends impacting Canada's cyber threat landscape that we raised in previous NCTAs remain relevant today. These trends continue to evolve over time in light of geopolitical, technological, and threat actor developments. For example:
https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026#section3

Redline, Meta Infostealer Malware Operations Seized By Police
Bleeping Computer, 10/28/2024

The Dutch National Police seized the network infrastructure for the Redline and Meta infostealer malware operations in "Operation Magnus," warning cybercriminals that their data is now in the hands of law enforcement. Operation Magnus was announced on a dedicated website that disclosed the disruption of the Redline and Meta operations, stating that legal actions based on the seized data are currently underway. "On the 28th of October 2024 the Dutch National Police, working in close cooperation with the FBI and other partners of the international law enforcement task force Operation Magnus, disrupted operation of the Redline and Meta infostealers," reads a short announcement on the Operation Magnus site. https://www.bleepingcomputer.com/news/legal/redline-meta-infostealer-malware-operations-seized-by-police/

How To Build A Next-Generation Of Railway Cybersecurity
Railway Technology, 11/4/2024

The railways are a pivotal part of the UK's infrastructure. The most recent Office for Road and Rail figures recorded a total of 420 million journeys made by passengers in Great Britain from April to June 2024, up 7% from the same period in 2023. Rail makes a huge contribution to the UK's economic productivity and connectivity. With many parts of the network now full at peak times, new capacity is urgently needed, alongside making existing operations more resilient and efficient. One way this is happening is through digital transformation. With modern signalling and train control capabilities, such as Connected Driver Advisory Systems (CDAS) and Traffic Management (TM) https://www.railway-technology.com/comment/how-to-build-a-next-generation-of-railway-cybersecurity/

1,000+ Web Shops Infected By "Phish 'n Ships" Criminals Who Create Fake Product Listings For In-Demand Products
Malwarebytes Labs, 11/1/2024

Researchers at the Satori Threat Intelligence and Research team have published their findings about a group of cybercriminals that infect legitimate web shops to create and promote fake product listings. The threat, dubbed "Phish 'n Ships" by the researchers, reportedly infected more than 1,000 websites and built 121 fake web stores to trick consumers. Estimated losses are in the region of tens of millions of dollars over the past five years. The group infected legitimate web shops with a malicious payload that would redirect visitors to web shops under their own control. While visiting such an affected web shop the visitor would be served fake product listings. When they clicked on the link for that item, hundreds of thousands of victims were redirected. https://www.malwarebytes.com/blog/news/2024/11/1000-web-shops-infected-by-phish-n-ships-criminals-who-create-fake-product-listings-for-in-demand-products

Autonomous Discovery of Critical Zero-Days
Zero Path, 10/29/2024

AI-driven 0-day detection is here. AI-assisted security research has been quietly advancing since early 2023, when AIxCC researchers demonstrated the first practical applications of LLM-powered vulnerability detection in AI systems. Modern LLMs have been used to improve the accuracy of detections of existing classes of web issues (XSS, SQLi, CSRF) and find business logic and authentication problems that were previously undetectable by SAST. Since July 2024, ZeroPath is taking a novel approach combining deep program analysis with adversarial AI agents for validation. Our methodology has uncovered numerous critical vulnerabilities in production systems, including several that traditional Static Application Security Testing (SAST) tools were ill-equipped to find. This post provides a technical deep-dive into our research methodology and a living summary of the bugs found in popular open-source tools. https://zeropath.com/blog/0day-discoveries

Supply Chain Security Is National Security: Cyber, Physical, and Personnel Protections
JDSUPRA, 10/30/2024

Company supply chain security efforts target three types of risks: Cyber Threats, Physical Security Threats, and Personnel Threats. This article surveys certain federal programs targeting historic and emerging threats within these risk categories together with the corresponding regulatory requirements. This simple three-part construct for assessing categories of threat applies to all asset and non-asset operations. It helps to manage risk assessments, deployment of resources, incident response, and corrective actions in the context of national security. Its value extends well beyond minimum regulatory compliance. https://www.jdsupra.com/legalnews/supply-chain-security-is-national-4984096/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Cybercriminals Use Webflow to Deceive Users into Sharing Sensitive Login Credentials -*** Cybersecurity researchers have warned of a spike in phishing pages created using a website builder tool called Webflow, as threat actors continue to abuse legitimate services like Cloudflare and Microsoft Sway to their advantage. https://thehackernews.com/2024/10/cybercriminals-use-webflow-to-deceive.html
- ***Russian Malware Campaign Targets Ukrainian Recruits Via Telegram -*** Russian threat actors are targeting the devices of Ukrainian military recruits in a malware campaign delivered via Telegram, a new analysis by Google has found. The group, tracked as UNC5812, is a suspected Russian hybrid espionage and influence operation. In the new campaign, discovered in September 2024, the attackers attempt to deliver Windows and Android malware to the Ukrainian military recruits using a Telegram persona named "Civil Defense." https://www.infosecurity-magazine.com/news/russian-malware-ukrainian-recruits/
- ***Fog and Akira ransomware attacks exploit SonicWall VPN flaw CVE-2024-40766*** - Fog and Akira ransomware operators are exploiting SonicWall VPN flaw CVE-2024-40766 to breach enterprise networks. https://securityaffairs.com/170359/cyber-crime/fog-akira-ransomware-sonicwall-vpn-flaw.html
- ***Black Basta Operators Phish Employees Via Microsoft Teams*** - Black Basta ransomware affiliates are still trying to trick enterprise employees into installing remote access tool by posing as help desk workers, now also via Microsoft Teams. https://www.helpnetsecurity.com/2024/10/28/black-basta-operators-phish-employees-via-microsoft-teams/
- ***Windows 'Downdate' Attack Reverts Patched PCs to a Vulnerable State*** -Fully patched Windows 11 systems are vulnerable to attacks that allow an adversary to install custom rootkits that can neutralize endpoint security mechanisms, hide malicious processes and network activity, maintain persistence and stealth on a compromised system, and more. https://www.darkreading.com/application-security/windows-downdate-attack-patched-pcs-vulnerable-state

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Cyber Attack Wipes Out DHL Delivery Tracking Systems Causing Issues For Nisa Retailers*** –DHL is suffering from a major cyber-attack at a partnered tech firm, wiping out its delivery tracking systems for stores, according to Nisa. In messages shared with Better Retailing, convenience group Nisa warned its retailers on the 31 October: "the DHL delivery tracking solution has encountered a cyber incident this morning that has affected all their systems globally." https://www.betterretailing.com/dhl-cyber-attack/
- ***Tens Of Thousands Of Taxpayer Accounts Hacked As CRA Repeatedly Paid Out Millions In Bogus Refunds*** - At the height of this year's tax season, the Canada Revenue Agency discovered that hackers had obtained confidential data used by one of the country's largest tax preparation firms, H&R Block Canada. https://www.cbc.ca/news/canada/canada-revenue-agency-taxpayer-accounts-hacked-1.7363440
- ***California Court Suffering From Tech Outages After Cyberattack*** - The San Joaquin County Superior Court said nearly all of its digital services have been knocked offline due to a cyberattack that began earlier this week. The court first warned the county's nearly 800,000 residents of technology issues on Wednesday before admitting that it was a cybersecurity incident on Thursday. https://therecord.media/california-court-suffering-from-tech-outages-cyberattack
- ***Italian Politicians Express Alarm at Latest Data Breach Allegedly Affecting 800,000 Citizens*** - Italian politicians called Monday for better protection of citizens' online data following a probe into a hacking scheme that allegedly breached law enforcement, tax authority and other sensitive public data. https://www.securityweek.com/italian-politicians-express-alarm-at-latest-data-breach-allegedly-affecting-800000-citizens/

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. PTZOptics PT30X-SDI/NDI Cameras –
    a. https://www.cve.org/CVERecord?id=CVE-2024-8957
    b. https://www.cve.org/CVERecord?id=CVE-2024-8956

SUSE Security Updates

1. gcc13 - https://www.suse.com/support/update/announcement/2024/suse-ru-20243761-2
2. openssl-1_1 –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20243905-1
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20243904-1
3. Rust - https://www.suse.com/support/update/announcement/2024/suse-ru-20243903-1
4. Shim - https://www.suse.com/support/update/announcement/2024/suse-ru-20243902-1
5. Protobuf –
    a. https://www.suse.com/support/update/announcement/2024/suse-ru-20243901-1
    b. https://www.suse.com/support/update/announcement/2024/suse-ru-20243900-1
6. MozillaFirefox –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20243899-1
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20243898-1
7. Shadow - https://www.suse.com/support/update/announcement/2024/suse-ru-20243897-1
8. openCryptoki –
    a. https://www.suse.com/support/update/announcement/2024/suse-ru-20243895-1
    b. https://www.suse.com/support/update/announcement/2024/suse-ru-20243894-1
9. Python-redis - https://www.suse.com/support/update/announcement/2024/suse-ou-20243893-1
10. Python-responses - https://www.suse.com/support/update/announcement/2024/suse-ru-20243892-1
11. Libkdumpfile - https://www.suse.com/support/update/announcement/2024/suse-ru-20243891-1
12. Wget-
    a. https://www.suse.com/support/update/announcement/2024/suse-ru-20243890-1
    b. https://www.suse.com/support/update/announcement/2024/suse-ru-20243888-1
13. Lvm2 –
    a. https://www.suse.com/support/update/announcement/2024/suse-ru-20243887-1
    b. https://www.suse.com/support/update/announcement/2024/suse-ru-20243886-1
14. Util-linux - https://www.suse.com/support/update/announcement/2024/suse-ru-20243237-2

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Fedora Security Advisories

1. Chromium –
    a. https://lwn.net/Articles/996869
    b. https://lwn.net/Articles/996868
    c. https://lwn.net/Articles/996867
2. Webkitgk - https://lwn.net/Articles/996875

Debian Security Advisories

1. Chromium - https://lists.debian.org/debian-security-announce/2024/msg00216.html

Check Point Security Advisories

1. Progress WhatsUp - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1030.html
2. RoundCube - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0974.html
3. Zyxel - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2022-2139.html
4. Cacti - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0967.html

Red Hat Security Advisories

1. xorg-x11-server and xorg-x11-server-Xwayland - https://access.redhat.com/errata/RHSA-2024:8798
2. openexr - https://access.redhat.com/errata/RHSA-2024:8800

Ubuntu Security Notices

1. Linux kernel –
    a. https://ubuntu.com/security/notices/USN-7089-2
    b. https://ubuntu.com/security/notices/USN-7088-2

Zero Day Initiative Advisories & Updates

1. Autodesk AutoCAD - https://www.zerodayinitiative.com/advisories/ZDI-24-1452/

OTHER

1. TOR Virtual Network Tunneling Tool 0.4.8.13 - https://packetstormsecurity.com/files/182470/tor-0.4.8.13.tar.gz