Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 13, 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

Delivering Results For America USDOT Progress Report: 2021–2023

Delivering Results for America describes the progress that the Department has made addressing the strategic goals and challenges facing our transportation system. Boosted by historic levels of funding provided by the Bipartisan Infrastructure Law, the Department has made great strides towards transforming our transportation system – making transportation safer, more reliable, more sustainable, and more affordable for travelers across our nation. Even as we celebrate the many milestones highlighted in this report, we continue to work tirelessly to stand up new programs and policies and get funding out to communities as swiftly and efficiently as possible. Working together with our partners across the nation, we strive to deliver the world's leading transportation system.
https://www.transportation.gov/sites/dot.gov/files/2024-02/USDOTAccomplishmentsProgressReport2021%E2%80%932023.pdf

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- CISA, FBI, NSA, and International Partners Release Joint Advisory on 2023 Top Routinely Exploited Vulnerabilities
- FBI Seeks Public Help to Identify Chinese Hackers Behind Global Cyber Intrusions
- Cyber Resilience Takes Centre Stage At Rail Industry Conference In London
- Attackers Breach IT-Based Networks Before Jumping to ICS/OT Systems
- Breaking the (Supply) Chain: The Macroeconomic Stakes of Cybersecurity in Fleet Telematics
- Microchip Technology Reports $21.4 Million Cost From Ransomware Attack
- Why SEBI's New Guidelines Make Cyber Threat Intelligence Essential for Security Teams

Emerging Threats & Vulnerabilities

- Beware of Phishing Emails Delivering Backdoored Linux VMs!
- DocuSign Abused to Deliver Fake Invoices
- Hackers Increasingly Use Winos4.0 Post-Exploitation Kit In Attacks
- Synology Urges Patch for Critical Zero-Click RCE Flaw Affecting Millions of NAS Devices
- ClickFix Exploits Users with Fake Errors and Malicious Code

Attacks, Breaches, & Leaks

- Cactus Ransomware Hits Lumiplan in Major Cyberattack
- Dynamic Systems Data Breach
- Radwan Cyber Pal Hacker Group Alleges Access to Sensitive Data of Israeli Soldiers and Settlers
- HIBP notifies 57 million people of Hot Topic data breach
- Debt Relief Firm Forth Discloses Data Breach Impacting 1.5 Million People

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, FBI, NSA, and International Partners Release Joint Advisory on 2023 Top Routinely Exploited Vulnerabilities
CISA, 11/12/2024

Today, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and international partners released joint Cybersecurity Advisory, 2023 Top Routinely Exploited Vulnerabilities. This advisory supplies details on the top Common Vulnerabilities and Exposures (CVEs) routinely exploited by malicious cyber actors and their associated Common Weakness Enumeration(s) (CWE) to help organizations better understand the impact of exploitation. International partners contributing to this advisory include: https://www.cisa.gov/news-events/alerts/2024/11/12/cisa-fbi-nsa-and-international-partners-release-joint-advisory-2023-top-routinely-exploited

FBI Seeks Public Help to Identify Chinese Hackers Behind Global Cyber Intrusions
The Hacker News, 11/5/2024

The U.S. Federal Bureau of Investigation (FBI) has sought assistance from the public in connection with an investigation involving the breach of edge devices and computer networks belonging to companies and government entities. "An Advanced Persistent Threat group allegedly created and deployed malware (CVE-2020-12271) as part of a widespread series of indiscriminate computer intrusions designed to exfiltrate sensitive data from firewalls worldwide," the agency said. "The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions." The development comes in the aftermath of a series of reports published by cybersecurity vendor Sophos chronicling a set of campaigns between 2018 and 2023 that exploited its edge infrastructure appliances to deploy custom malware or repurpose them as proxies to fly under the radar.
https://thehackernews.com/2024/11/fbi-seeks-public-help-to-identify.html

Cyber Resilience Takes Centre Stage At Rail Industry Conference In London
Global Railway Review, 11/12/2024

Northern has announced that more than 100 rail industry professionals had gathered in London on 11 November 2024, for a conference focused on strengthening cyber resilience within the sector. The event, organised by Northern, aimed to bring together key players in rail safety and digital security to discuss strategies for mitigating cyber threats to the railway network. Keynote speaker Mark Philips, CEO of the Rail Safety & Standards Board (RSSB), emphasised the importance of proactive cyber risk management, stating, “Don’t plan for if, plan for when,” he urged delegates,
https://www.globalrailwayreview.com/news/179920/cyber-resilience-takes-centre-stage-rail-industry-conference-in-london/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Attackers Breach IT-Based Networks Before Jumping to ICS/OT Systems
Dark Reading, 11/6/2024

Attacks against industrial-control systems (ICS) and operational technology (OT) systems are increasing, as adversaries find weaknesses in IT networks that allow them to move into OT networks, according to a recent report from the SANS Institute. The "State of ICS/OT Cybersecurity 2024" report is based on responses from cybersecurity professionals in various critical-infrastructure sectors. More non-ransomware incidents (74.4%) were reported than ransomware (11.7%) over the past year, according to the report. Other initial attack vectors involved in OT/ICS incidents include compromising these systems by use of external remote services (23.7%) or Internet-accessible devices (23.7%), compromising employee workstations (20.3%) and removable media (20.3%), and a supply chain compromise (20.3%). https://www.darkreading.com/ics-ot-security/attackers-breach-network-provider-ot-ics-network

Breaking the (Supply) Chain: The Macroeconomic Stakes of Cybersecurity in Fleet Telematics
Upstream, 11/7/2024

In an era where smart mobility and connected technologies are revolutionizing the automotive industry, reliance on telematics and IoT devices to manage fleet operations has surged. These advancements streamline operations and enhance fleet performance but also introduce new vulnerabilities. Recent cyber attacks, such as those involving a prominent UK-based telematics vendor and a US-based electronic logging (ELDs) and inventory management IoT provider, demonstrate how disruptions to telematics systems can create ripple effects across industries and economies. These incidents underscore the macroeconomic stakes in securing the automotive and mobility ecosystem against cyber threats. https://upstream.auto/blog/cybersecurity-risks-in-fleet-telematics/

Microchip Technology Reports $21.4 Million Cost From Ransomware Attack
Security Week, 11/6/2024

The incident came to light in August, when the US-based semiconductor supplier found suspicious activity on its network. The intrusion resulted in disruptions at some of Microchip's manufacturing facilities. The Play ransomware group took credit for the attack roughly one week later, claiming to have stolen gigabytes of data. The ransomware gang has published files allegedly stolen from the company, which indicates that Microchip refused to pay a ransom. The hackers have made available a 4 Gb archive file allegedly containing Microchip data. They claim the leaked data includes personal data, client documents, and files related to budget, payroll, accounting, contracts, taxes, and finances. https://www.securityweek.com/microchip-technology-reports-21-4-million-cost-from-ransomware-attack/

Why SEBI's New Guidelines Make Cyber Threat Intelligence Essential for Security Teams
The Cyber Express, 11/12/2024

Beginning in January, investment and financial firms that fall under the Securities and Exchange Board of India (SEBI) will face some of the most comprehensive cybersecurity regulations on the planet. SEBI's 205-page Cybersecurity and Cyber Resilience Framework (CSCRF) for Regulated Entities (REs) was published in August and will take effect on Jan. 1, 2025 for organizations that are already under existing SEBI cybersecurity circulars, and April 1, 2025 for those that will be covered by CSCRF for the first time. The document is a well thought-out blueprint for strong cybersecurity – and requires investment firms, asset managers and other REs to adopt stringent controls and practices that culminate in in-depth auditing and reporting requirements. https://thecyberexpress.com/sebi-new-guidelines-make-cti-essential/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Beware of Phishing Emails Delivering Backdoored Linux VMs! -*** Unknown attackers are trying to trick Windows users into spinning up a custom Linux virtual machine (VM) with a pre-configured backdoor, Securonix researchers have discovered. https://www.helpnetsecurity.com/2024/11/05/phishing-oneamerica-survey-linux-vm-backdoor/
- ***DocuSign Abused to Deliver Fake Invoices –*** Unlike traditional phishing, which involves spoofed email messages mimicking known brands aimed at harvesting credentials or installing malware, this campaign relies on the trusted e-signing service to deliver malicious content. https://www.securityweek.com/docusign-apis-abused-to-deliver-fake-invoices/
- ***Hackers Increasingly Use Winos4.0 Post-Exploitation Kit In Attacks*** - Hackers are increasingly targeting Windows users with the malicious Winos4.0 framework, distributed via seemingly benign game-related apps. The toolkit is the equivalent of Sliver and Cobalt Strike post-exploitation frameworks and it was documented by Trend Micro this summer in a report on attacks against Chinese users. https://www.bleepingcomputer.com/news/security/hackers-increasingly-use-winos40-post-exploitation-kit-in-attacks/
- ***Synology Urges Patch for Critical Zero-Click RCE Flaw Affecting Millions of NAS Devices*** -Taiwanese network-attached storage (NAS) appliance maker Synology has addressed a critical security flaw impacting DiskStation and BeePhotos that could lead to remote code execution. https://thehackernews.com/2024/11/synology-urges-patch-for-critical-zero.html
- ***ClickFix Exploits Users with Fake Errors and Malicious Code*** - A new social engineering tactic, known as ClickFix, has emerged, using deceptive error messages to prompt users to run harmful code. The Sekoia Threat Detection & Research (TDR) team has recently detailed this tactic – first discovered by Proofpoint in March – in a new report published earlier today. This approach, called ClearFake, encourages users to copy and execute malicious PowerShell commands, enabling cybercriminals to infect users' devices. https://www.infosecurity-magazine.com/news/clickfix-fake-errors-malicious-code

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***Cactus Ransomware Hits Lumiplan in Major Cyberattack*** – Recently, the Cactus ransomware group has taken responsibility for a cyberattack on Lumiplan, a prominent French company known for its real-time communication solutions. Lumiplan excels in digital signage and passenger information systems, primarily serving the transportation sector to enhance mobility and passenger experiences across various industries. https://ransomwareattacks.halcyon.ai/attacks/cactus-ransomware-hits-lumiplan-in-major-cyberattack
- ***Dynamic Systems Data Breach*** - Dynamic Systems specializes in providing tailored technology advisory and execution services to government agencies, focusing on infrastructure modernization, cloud migration, and addressing critical IT challenges in the public sector. https://www.breachsense.com/breaches/dynamic-systems-data-breach/
- ***Radwan Cyber Pal Hacker Group Alleges Access to Sensitive Data of Israeli Soldiers and Settlers*** - A new wave of cyberattacks has started targeting Israel, with an anti-Israel hacker group calling itself "Radwan Cyber Pal" claiming responsibility for a breach of the Ministry of National Security. https://thecyberexpress.com/radwan-cyber-pal-alleged-cyberattack/
- ***HIBP notifies 57 million people of Hot Topic data breach*** - Have I Been Pwned warns that an alleged data breach exposed the personal information of 56,904,909 accounts for Hot Topic, Box Lunch, and Torrid customers. https://www.securityweek.com/law-firm-data-breach-impacts-300000-presbyterian-healthcare-patients/
- ***Debt Relief Firm Forth Discloses Data Breach Impacting 1.5 Million People*** - Debt relief solutions provider Forth (Set Forth) is notifying 1.5 million individuals that their personal information was compromised in a May 2024 data breach. https://www.securityweek.com/debt-relief-firm-forth-discloses-data-breach-impacting-1-5-million-people/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. Qemu - https://www.suse.com/support/update/announcement/2024/suse-ru-20243981-1
2. Strongswan - https://www.suse.com/support/update/announcement/2024/suse-ru-20243982-1
3. Linux Kernel –
    a. https://www.suse.com/support/update/announcement/2024/suse-su-20243983-1
    b. https://www.suse.com/support/update/announcement/2024/suse-su-20243984-1
    c. https://www.suse.com/support/update/announcement/2024/suse-su-20243985-1
    d. https://www.suse.com/support/update/announcement/2024/suse-su-20243986-1
4. java-1_8_0-openjdk - https://www.suse.com/support/update/announcement/2024/suse-su-20243987-1

Fedora Security Advisories

1. chromium –
    a. https://lwn.net/Articles/998018
    b. https://lwn.net/Articles/998018
2. golang-github-nvidia-container-toolkit –
    a. https://lwn.net/Articles/998020
    b. https://lwn.net/Articles/998019

Mageia Security Advisories

1. qbittorrent - http://advisories.mageia.org/MGASA-2024-0359.html
2. curl - http://advisories.mageia.org/MGASA-2024-0360.html
3. php-tcpdf - http://advisories.mageia.org/MGASA-2024-0361.html
4. expat - http://advisories.mageia.org/MGASA-2024-0362.html

Check Point Security Advisories

1. OpenSSH - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2019-3233.html
2. Ivanti - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1051.html
3. DrayTek - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-0892.html
4. Citrix - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1064.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Red Hat Security Advisories

1. grafana-pcp - https://access.redhat.com/errata/RHSA-2024:9551
2. thunderbird - https://access.redhat.com/errata/RHSA-2024:9552
3. webkit2gtk3 - https://access.redhat.com/errata/RHSA-2024:9553
4. firefox - https://access.redhat.com/errata/RHSA-2024:9554
5. NetworkManager-libreswan - https://access.redhat.com/errata/RHSA-2024:9555
6. Libsoup - https://access.redhat.com/errata/RHSA-2024:9559

Other

1. Chrome Beta for iOS - https://chromereleases.googleblog.com/2024/11/chrome-beta-for-ios-update_13.html