Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

November 19, 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

If You See Something, Say Something®

"If You See Something, Say Something®" is a national campaign that raises public awareness of the signs of terrorism and terrorism-related crime, and how to report suspicious activity to state and local law enforcement. We all play a role in keeping our communities safe. It's easy to be distracted during our daily routines such as going to work, school, or the grocery store, but as you're going about your day, if you see something that doesn't seem quite right, say something. Your tip could help save lives. https://www.dhs.gov/see-something-say-something

Additional Resources:

- Recognize Suspicious Activity: https://www.dhs.gov/see-something-say-something/recognize-the-signs
- How to Report Suspicious Activity: https://www.dhs.gov/see-something-say-something/how-to-report-suspicious-activity

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

AT-A-GLANCE

Executive News

- The FBI Warns of a Surge in Fake Emergency Data Requests
- 300 Drinking Water Systems in U.S. Exposed to Disruptive, Damaging Hacker Attacks
- Volt Typhoon Rebuilds Malware Botnet Following Fbi Disruption
- OvrC Platform Vulnerabilities Expose IoT Devices to Remote Attacks and Code Execution
- Amazon MOVEit Leaker Claims to Be Ethical Hacker
- How Technology Is Reinventing The Trucking Industry For The 21st Century
- How To Remove The Cybersecurity Gridlock From The Nation's Energy Lifelines

Emerging Threats & Vulnerabilities

- Microsoft Bookings Flaw Enables Account Hijacking and Impersonation
- New Citrix Zero-Day Vulnerability Allows Remote Code Execution
- SAP Patches High-Severity Vulnerability in Web Dispatcher
- New Phishing Tool GoIssue Targets GitHub Developers in Bulk Email Campaigns
- D-Link Won't Fix Critical Bug In 60,000 Exposed Eol Modems

Attacks, Breaches, & Leaks

- ADT Freight Services Listed As Alleged Victim By Sarcoma Ransomware Gang
- IP Spoofing Attack Tried to Disrupt Tor Network
- Space Tech Giant Maxar Confirms Attackers Accessed Employee Data
- Equinox Notifies Clients And Employees Of April Data Security Incident

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

The FBI Warns of a Surge in Fake Emergency Data Requests
In Cyber News, 11/15/2024

On November 4, 2024, the FBI issued a warning about a sharp increase in the sale of credentials for police and government agency email accounts on criminal forums. These credentials are often accompanied by forged legal documents, such as warrants or subpoenas. Together, they enable the fraudulent submission of fake emergency data requests to U.S. companies. “Cybercriminals gain access to compromised email accounts of U.S. and foreign government entities and use them to make fraudulent emergency data requests to U.S.-based companies, exposing customer personal information to subsequent criminal use,” the FBI summarized. https://incyber.org/en/article/the-fbi-warns-of-a-surge-in-fake-emergency-data-requests/

300 Drinking Water Systems in U.S. Exposed to Disruptive, Damaging Hacker Attacks
Security Week, 11/18/2024

A passive assessment of security defects in 1,062 drinking water systems that serve over 193 million individuals has revealed that a quarter of them could potentially fall victim to attacks leading to functionality loss, denial-of-service (DoS) conditions, and customer information compromise. The assessment covered five cybersecurity categories, namely email security, IT hygiene, vulnerabilities, adversarial threat, and malicious activity, and rated the identified weaknesses with critical to low scores, based on their potential impact. As of October 2024, 97 of the assessed water systems, which serve approximately 27 million individuals, contained critical and high-severity issues, OIG’s report (PDF) shows. https://www.securityweek.com/300-drinking-water-systems-in-us-exposed-to-disruptive-damaging-hacker-attacks/

Volt Typhoon Rebuilds Malware Botnet Following Fbi Disruption
Bleeping Computer, 11/12/2024

The Chinese state-sponsored hacking group Volt Typhoon has begun to rebuild its "KV-Botnet" malware botnet after it was disrupted by law enforcement in January, according to researchers from SecurityScorecard. Volt Typhoon is a Chinese state-sponsored cyberespionage threat group that is believed to have infiltrated critical U.S. infrastructure, among other networks worldwide, since at least five years ago. Their primary strategy involves hacking SOHO routers and networking devices, such as Netgear ProSAFE firewalls, Cisco RV320s, DrayTek Vigor routers, and Axis IP cameras, to install custom malware that establishes covert communication and proxy channels and maintain persistent access to targeted networks. https://www.bleepingcomputer.com/news/security/volt-typhoon-rebuilds-malware-botnet-following-fbi-disruption/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

OvrC Platform Vulnerabilities Expose IoT Devices to Remote Attacks and Code Execution
The Hacker News, 11/14/2024

A security analysis of the OvrC cloud platform has uncovered 10 vulnerabilities that could be chained to allow potential attackers to execute code remotely on connected devices. "Attackers successfully exploiting these vulnerabilities can access, control, and disrupt devices supported by OvrC; some of those include smart electrical power supplies, cameras, routers, home automation systems, and more," Claroty researcher Uri Katz said in a technical report. Snap One's OvrC, pronounced "oversee," is advertised as a "revolutionary support platform" that enables homeowners and businesses to remotely manage, configure, and troubleshoot IoT devices on the network.
https://thehackernews.com/2024/11/ovrc-platform-vulnerabilities-expose.html

Amazon MOVEit Leaker Claims to Be Ethical Hacker
Infosecurity Magazine, 11/13/2024

A threat actor who posted 2.8 million lines of Amazon employee data last week has taken to the dark web to claim they are doing so to raise awareness of poor security practice. The individual, who goes by the online moniker “Nam3L3ss,” claimed in a series of posts to have obtained data from 25 organizations whose data was compromised via last year’s MOVEit exploit. According to Hudson Rock, which verified the data, these organizations include McDonald’s, Charles Schwab, Lenovo, Delta Airlines, HSBC and Amazon – with an estimated five million records leaked so far. “This structured data reveals not only contact information but also sensitive details about organizational roles and department assignments, potentially opening doors to social engineering and other security threats,” the security vendor warned. https://www.infosecurity-magazine.com/news/amazon-moveit-leaker-claims/

How Technology Is Reinventing The Trucking Industry For The 21st Century
Fleet Owner, 11/18/2024

Fleet managers in trucking aren’t just dispatchers anymore; they’re data interpreters, efficiency experts, and safety strategists. In an industry where fuel costs swing unpredictably, regulatory compliance is a moving target, and safety is paramount, technology provides an edge that’s hard to ignore. From route optimization and telematics to predictive maintenance, these tools offer more than just improvements; they’re giving fleets a way to stay competitive and cost-effective. Delivering a load of goods used to be about getting from Point A to Point B. Today, it’s about getting there as efficiently as possible while dodging traffic, road closures, and weather disruptions.
https://www.fleetowner.com/perspectives/ideaxchange/blog/55243015/how-technology-is-reinventing-the-trucking-industry-for-the-21st-century

How To Remove The Cybersecurity Gridlock From The Nation's Energy Lifelines
Cyber Scoop, 11/19/2024

In a world where every digital connection has the potential to be a vulnerability, the stakes for cybersecurity have never been higher. The recent statement from National Security Advisor Jake Sullivan on supply chain security brings into sharp focus the escalating threats faced by critical infrastructure operators, particularly the energy sector. For the United States, securing this sector is not just a matter of national interest; it's a strategic necessity that reverberates across global markets. As the energy sector becomes increasingly intertwined with complex networks of software and IT vendors, the risk of a cyber incident grows exponentially. The integration of industrial control systems (ICS) and energy automation offers operational benefits but also opens doors to significant vulnerabilities.
https://cyberscoop.com/cybersecurity-energy-sector-supply-chain-risks-brian-harrell-sachin-bansal/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Microsoft Bookings Flaw Enables Account Hijacking and Impersonation*** - A vulnerability in Microsoft Bookings can expose your organization to serious security risks. Learn how attackers can exploit this flaw to create convincing impersonations, launch phishing attacks, and compromise sensitive data. https://hackread.com/microsoft-bookings-flaw-account-hijack-impersonate/
- ***New Citrix Zero-Day Vulnerability Allows Remote Code Execution*** - A new zero-day vulnerability in Citrix's Session Recording Manager can be exploited to enable unauthenticated remote code execution (RCE) against Citrix Virtual Apps and Desktops, according to watchTowr. https://www.infosecurity-magazine.com/news/new-citrix-zeroday-vulnerability/
- ***SAP Patches High-Severity Vulnerability in Web Dispatcher -*** Marked as 'high priority', the second most severe rating in SAP's playbook, the most important of these notes resolves a high-severity vulnerability in Web Dispatcher, the appliance that distributes incoming requests to the adequate SAP instances. https://www.securityweek.com/sap-patches-high-severity-vulnerability-in-web-dispatcher/
- ***New Phishing Tool GoIssue Targets GitHub Developers in Bulk Email Campaigns –*** Cybersecurity researchers are calling attention to a new sophisticated tool called GoIssue that can be used to send phishing messages at scale targeting GitHub users. https://thehackernews.com/2024/11/new-phishing-tool-goissue-targets.html
- ***D-Link Won't Fix Critical Bug In 60,000 Exposed Eol Modems -*** Tens of thousands of exposed D-Link routers that have reached their end-of-life are vulnerable to a critical security issue that allows an unauthenticated remote attacker to change any user's password and take complete control of the device. https://www.bleepingcomputer.com/news/security/d-link-wont-fix-critical-bug-in-60-000-exposed-eol-modems/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***ADT Freight Services Listed As Alleged Victim By Sarcoma Ransomware Gang -*** The gang listed ADT Freight Services on 14 November; however, Sarcoma seems to have gotten away with little in the way of digital loot. https://www.cyberdaily.au/security/11362-exclusive-adt-freight-services-listed-as-alleged-victim-by-sarcoma-ransomware-gang
- ***IP Spoofing Attack Tried to Disrupt Tor Network*** - The Tor Project said the attack started on October 20, when Tor directory authorities, the critical components responsible for managing and maintaining the list of Tor relays, started getting complaints alleging that their servers had been conducting port scanning. https://www.securityweek.com/ip-spoofing-attack-tried-to-disrupt-tor-network/
- ***Space Tech Giant Maxar Confirms Attackers Accessed Employee Data*** - "Our information security team discovered that a hacker using a Hong Kong-based IP address targeted and accessed a Maxar system containing certain files with employee personal data," the company's data breach notice says. https://www.helpnetsecurity.com/2024/11/19/maxar-breach/
- ***Equinox Notifies Clients And Employees Of April Data Security Incident*** - On November 15, Equinox notified clients and staff members about what they described as a data security incident on April 29. With a little digging, DataBreaches realized that it was an attack by LockBit3.0. https://databreaches.net/2024/11/18/ny-equinox-notifies-clients-and-employees-of-april-data-security-incident/

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. MITSUBISHI ELECTRIC- HTTPS://WWW.CISA.GOV/NEWS-EVENTS/ICS-ADVISORIES/ICSA-24-324-01

SUSE Security Updates

1. BEA-STAX, XSTREAM - HTTPS://WWW.SUSE.COM/SUPPORT/UPDATE/ANNOUNCEMENT/2024/SUSE-SU-20244037-1
2. LINUX KERNEL - HTTPS://WWW.SUSE.COM/SUPPORT/UPDATE/ANNOUNCEMENT/2024/SUSE-SU-20244037-1

Check Point Security Advisories

1. 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
2. KEMP - HTTPS://ADVISORIES.CHECKPOINT.COM/DEFENSE/ADVISORIES/PUBLIC/2024/CPAI-2024-0143.HTML
3. HP OPENVIEW - HTTPS://ADVISORIES.CHECKPOINT.COM/DEFENSE/ADVISORIES/PUBLIC/2024/CPAI-2011-0793.HTML

Red Hat Security Advisories

1. OPENSHIFT CONTAINER PLATFORM 4.17.5 –
    a. HTTPS://ACCESS.REDHAT.COM/ERRATA/RHSA-2024:9610
    b. HTTPS://ACCESS.REDHAT.COM/ERRATA/RHSA-2024:9610

Ubuntu Security Notices

1. PYTHON –
    a. HTTPS://UBUNTU.COM/SECURITY/NOTICES/USN-7015-5
    b. HTTPS://UBUNTU.COM/SECURITY/NOTICES/USN-7116-1

2. WAITRESS – HTTPS://UBUNTU.COM/SECURITY/NOTICES/USN-7115-1
3. NEEDRESTART - HTTPS://UBUNTU.COM/SECURITY/NOTICES/USN-7117-1

ZERO DAY INITIATIVE ADVISORIES & UPDATES

1. SIEMENS –
    a. HTTPS://WWW.ZERODAYINITIATIVE.COM/ADVISORIES/ZDI-24-1527/
    b. HTTPS://WWW.ZERODAYINITIATIVE.COM/ADVISORIES/ZDI-24-1526/
    c. HTTPS://WWW.ZERODAYINITIATIVE.COM/ADVISORIES/ZDI-24-1525/
    d. HTTPS://WWW.ZERODAYINITIATIVE.COM/ADVISORIES/ZDI-24-1523/