Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

December 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.

AT-A-GLANCE

Executive News

- CISA and ONCD Publish Guide to Strengthen Cybersecurity of Grant-Funded Infrastructure Projects
- Amnesty Accuses Serbia of Tracking Journalists and Activists with Spyware
- Threats in Transit: Cyberattacks Disrupting the Transportation Industry
- Silent Threats: The Hidden Danger Of Machine Identities
- Ivanti Warns Of Maximum Severity Csa Auth Bypass Vulnerability
- What Consolidations Among Tech Providers Mean For Their Trucking Customers
- Email Security: Why Traditional Defenses Fall Short In Today's Threat Landscape

Emerging Threats & Vulnerabilities

- Dell Urges Immediate Update to Fix Critical Power Manager Vulnerability
- Cisco Says Flaws in Industrial Routers, BGP Tool Remain Unpatched 8 Months After Disclosure
- SAP fixed critical SSRF flaw in NetWeaver’s Adobe Document Services
- Hackers Weaponize Visual Studio Code Remote Tunnels for Cyber Espionage
- Sprawling 'Operation Digital Eye' Attack Targets European IT Orgs

Attacks, Breaches, & Leaks

- Qilin Ransomware Strikes Whitestown Highway Department
- 5 Million Payment Card Details Stolen In Painful Reminder To Monitor Christmas Spending
- Engineered Tower Solutions Data Breach
- UT Southwestern Medical Center has disclosed at least four breaches since July 2023. Is HHS investigating?
- SRP Federal Credit Union Ransomware Attack Impacts 240,000

EXECUTIVE NEWS

CISA and ONCD Publish Guide to Strengthen Cybersecurity of Grant-Funded Infrastructure Projects
CISA, 12/17/2024

The Cybersecurity and Infrastructure Security Agency (CISA) and Office of the National Cyber Director (ONCD) published a guide today with tools and resources to enable grant-making agencies to incorporate cybersecurity into their grant programs and to enable grant-recipients to build cyber resilience into their grant-funded infrastructure projects. This guide is for federal grant program managers, critical infrastructure owners and operators and organizations such as state, local, tribal, and territorial governments who subaward grant program funds, and grant program recipients. https://www.cisa.gov/news-events/news/cisa-and-oncd-publish-guide-strengthen-cybersecurity-grant-funded-infrastructure-projects

Amnesty Accuses Serbia of Tracking Journalists and Activists with Spyware
Infosecurity Magazine, 12/16/2024

The Serbian government is using advanced mobile forensics products from Israeli surveillance firm Cellebrite to spy on journalists and environmental and civil rights activists, according to an Amnesty International report. Amnesty shared findings from its Security Lab showing the use of spyware by the Serbian police forces and intelligence services in its report titled A Digital Prison: Surveillance and the suppression of civil society in Serbia, published on December 16. The report uncovered the use of NoviSpy, a previously unknown bespoke Android spyware tool. https://www.infosecurity-magazine.com/news/amnesty-accuses-serbia-spyware/

Threats in Transit: Cyberattacks Disrupting the Transportation Industry
CSA, 12/17/2024

The transportation industry is the lifeblood of the global economy—moving goods, people, and essential services across borders and cities. However, as the world becomes increasingly interconnected, so too does the vulnerability of this critical sector. Cybercriminals have zeroed in on transportation companies, knowing that even a brief disruption can cause far-reaching economic and logistical consequences. For example, freight shipping provider Estes Express Lines was targeted by a ransomware attack in October 2023 that forced the company to disable its internal IT systems for more than two and a half weeks. The attack also exposed the private data—including names, Social Security numbers, and other personal details—of 21,000 individuals. https://cloudsecurityalliance.org/blog/2024/12/17/threats-in-transit-cyberattacks-disrupting-the-transportation-industry#

Silent Threats: The Hidden Danger Of Machine Identities
SC Media, 12/12/2024

As non-human identities outnumber humans 45 to 1, enterprises face escalating security risks from unmonitored APIs, bots, and service accounts. Machine identities now outnumber humans in the digital world, but these silent gatekeepers are leaving enterprises dangerously exposed. APIs, bots, and service accounts power today's automation, yet they often go unnoticed, mismanaged, and unprotected—providing attackers with easy entry points. As businesses embrace advanced technologies, the hidden vulnerabilities in non-human identities (NHIs) are quickly becoming one of the biggest security risks in modern enterprises. https://www.scworld.com/feature/silent-threats-the-hidden-danger-of-machine-identities

Ivanti Warns Of Maximum Severity CSA Auth Bypass Vulnerability
Bleeping Computer, 12/10/2024

Today, Ivanti warned customers about a new maximum-severity authentication bypass vulnerability in its Cloud Services Appliance (CSA) solution. The security flaw (tracked as CVE-2024-11639 and reported by CrowdStrike's Advanced Research Team) enables remote attackers to gain administrative privileges on vulnerable appliances running Ivanti CSA 5.0.2 or earlier without requiring authentication or user interaction by circumventing authentication using an alternate path or channel. Ivanti advises admins to upgrade vulnerable appliances to CSA 5.0.3 using detailed information available in this support document. https://www.bleepingcomputer.com/news/security/ivanti-warns-of-maximum-severity-csa-auth-bypass-vulnerability/

What Consolidations Among Tech Providers Mean For Their Trucking Customers
CCJ, 12/15/2024

Bestpass-Fleetworthy, Drivewye, Empire, Zonar, GPS Trackit, Powerfleet and Fleet Complete. Those are just some of the technology companies that serve the trucking industry that have recently been involved in consolidations. One of the biggest of the year was Platform Science's announcement in September that it plans to acquire Trimble's telematics business, which was built in large part in 2011 when it acquired PeopleNet. That deal is expected to close in the first half of 2025. And additional deals could be on the horizon. https://www.ccjdigital.com/business/mergers-acquisitions/article/15710452/what-consolidations-among-tech-providers-mean-for-their-trucking-customers

Email Security: Why Traditional Defenses Fall Short In Today's Threat Landscape
Dark Reading, 12/11/2024

Despite decades of technological advancement, email remains the predominant attack vector for cybercriminals, with estimates suggesting that 80-90 percent of cyberattacks originate through email channels. While the cybersecurity industry has made significant strides in other areas, many businesses continue to rely on outdated email security measures that leave them vulnerable to increasingly sophisticated threats. This protection gap demands immediate attention from IT leaders. Traditional secure email gateways (SEGs) like Mimecast and Proofpoint have served as the backbone of organizational email security for years. https://betanews.com/2024/12/10/email-security-why-traditional-defenses-fall-short-in-todays-threat-landscape/

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***Dell Urges Immediate Update to Fix Critical Power Manager Vulnerability -*** A critical security flaw in Dell Power Manager has been discovered that could allow attackers to compromise your systems and execute arbitrary code. https://hackread.com/dell-urges-update-critical-power-manager-vulnerability/
- ***Cisco Says Flaws in Industrial Routers, BGP Tool Remain Unpatched 8 Months After Disclosure*** - Cisco's threat intelligence and research unit Talos has disclosed the details of several apparently unpatched vulnerabilities in an MC Technologies industrial router and the GoCast BGP tool. https://www.securityweek.com/cisco-says-flaws-in-industrial-routers-bgp-tool-remain-unpatched-8-months-after-disclosure/
- ***SAP fixed critical SSRF flaw in NetWeaver's Adobe Document Services -*** SAP has issued patches for 16 vulnerabilities, including a critical SSRF flaw in NetWeaver's Adobe Document Services. https://securityaffairs.com/171839/security/sap-fixed-critical-ssrf-flaw-netweaver.html
- ***Hackers Weaponize Visual Studio Code Remote Tunnels for Cyber Espionage –*** A suspected China-nexus cyber espionage group has been attributed to an attacks targeting large business-to-business IT service providers in Southern Europe as part of a campaign codenamed Operation Digital Eye. https://thehackernews.com/2024/12/hackers-weaponize-visual-studio-code.html
- ***Sprawling 'Operation Digital Eye' Attack Targets European IT Orgs –*** Details have emerged about a now-patched security flaw in the DeepSeek artificial intelligence (AI) chatbot that, if successfully exploited, could permit a bad actor to take control of a victim's account by means of a prompt injection attack. https://thehackernews.com/2024/12/researchers-uncover-prompt-injection.html

ATTACKS, BREACHES & LEAKS

- ***Qilin Ransomware Strikes Whitestown Highway Department -*** The Town of Whitestown Highway Department, a critical municipal entity in New York, has allegedly fallen victim to a ransomware attack orchestrated by the Qilin group. This incident underscores the vulnerabilities faced by governmental bodies in the digital age. https://www.halcyon.ai/attacks/qilin-ransomware-strikes-whitestown-highway-department
- ***5 Million Payment Card Details Stolen In Painful Reminder To Monitor Christmas Spending*** - This time, 5 million US credit cards and personal details were leaked online. The Leakd.com security team discovered that 5 terabytes of sensitive screenshots were exposed in a freely accessible Amazon S3 bucket. https://www.malwarebytes.com/blog/news/2024/12/5-million-payment-card-details-stolen-in-painful-reminder-to-monitor-christmas-spending
- ***Engineered Tower Solutions Data Breach -*** Engineered Tower Solutions provides comprehensive engineering services tailored to the telecommunications sector, specializing in the design, construction, and maintenance of wireless infrastructure. https://www.breachsense.com/breaches/engineered-tower-solutions-data-breach/
- ***UT Southwestern Medical Center has disclosed at least four breaches since July 2023. Is HHS investigating?*** - According to DataBreaches' count, UT Southwestern Medical Center in Texas has disclosed at least four breaches since July 2023. As a brief recap of the first three: https://databreaches.net/2024/12/13/ut-southwestern-medical-center-has-disclosed-at-least-four-breaches-since-july-2023-is-hhs-investigating/
- ***SRP Federal Credit Union Ransomware Attack Impacts 240,000*** - According to the credit union, a threat actor had access to its systems from at least September 5, 2024, until November 4, 2024, and "potentially acquired certain files from our network during that time". https://www.securityweek.com/srp-federal-credit-union-ransomware-attack-impacts-240000/

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

US CERT/ ICS CERT Alerts and Advisories

1. Hitachi –
    a. https://www.cisa.gov/news-events/ics-advisories/icsa-24-354-01
    b. https://www.cisa.gov/news-events/ics-advisories/icsa-24-354-02
2. Delta - https://www.cisa.gov/news-events/ics-advisories/icsa-24-354-03
3. Siemens - https://www.cisa.gov/news-events/ics-advisories/icsa-24-354-04
4. Tibbo - https://www.cisa.gov/news-events/ics-advisories/icsa-24-354-05
5. Schneider –
    a. https://www.cisa.gov/news-events/ics-advisories/icsa-24-354-06
    b. https://www.cisa.gov/news-events/ics-advisories/icsa-24-354-07
6. Ossur - https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-354-01

SUSE Security Updates

1. Linux Kernel – https://www.suse.com/support/update/announcement/2024/suse-su-20244387-1
2. Avahi - https://www.suse.com/support/update/announcement/2024/suse-su-20244386-1
3. Curl - https://www.suse.com/support/update/announcement/2024/suse-su-20243927-2
4. Glib2 - https://www.suse.com/support/update/announcement/2024/suse-su-20244051-2
5. release-notes-sles-for-sap - https://www.suse.com/support/update/announcement/2024/suse-ru-20244385-1
6. grub2 –
    a. https://www.suse.com/support/update/announcement/2024/suse-ru-20244384-1
    b. https://www.suse.com/support/update/announcement/2024/suse-ru-20244383-1
7. Quagga - https://www.suse.com/support/update/announcement/2024/suse-ru-20244382-1
8. net-snmp - https://www.suse.com/support/update/announcement/2024/suse-ru-20244381-1

Fedora Security Advisories

1. ColPack - https://lwn.net/Articles/1002875
2. golang-github-task - https://lwn.net/Articles/1002879
3. icecat - https://lwn.net/Articles/1002880
4. golang-github-chainguard-dev-git-urls - https://lwn.net/Articles/1002878
5. glibc - https://lwn.net/Articles/1002877
6. python3.13 - https://lwn.net/Articles/1002884
7. python-nbdime - https://lwn.net/Articles/1002882

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

Check Point Security Advisories

1. Cyberpanel - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1036.html
2. GitHub - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1160.html
3. Cacti - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1162.html
4. Apache - https://advisories.checkpoint.com/defense/advisories/public/2024/cpai-2024-1158.html

Red Hat Security Advisories

1. Satellite 6.16.1 Async - https://access.redhat.com/errata/RHSA-2024:11574
2. JBoss Enterprise Application Platform 8.0.5 - https://access.redhat.com/errata/RHSA-2024:11570

Ubuntu Security Notices

1. Kernel Live - https://ubuntu.com/security/notices/LSN-0108-1
2. DPDK - https://ubuntu.com/security/notices/USN-7178-1

Other

1. Chrome –
   a. https://chromereleases.googleblog.com/2024/12/extended-stable-updates-for-desktop_19.html

*** 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.