Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

Daily Open-Source Cyber Report

September 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.

AT-A-GLANCE

Executive News

- City Of Columbus Tries To Silence Security Researcher
- Iranian-Linked Hackers Collaborate With Ransomware Affiliates, Feds Say
- Censys Finds Hundreds of Exposed Servers as Volt Typhoon APT Targets Service Providers
- Researchers Find SQL Injection To Bypass Airport TSA Security Checks
- Hitachi Energy Vulnerabilities Plague SCADA Power Systems
- Published Vulnerabilities Surge by 43%
- Cyber Threats That Shaped The First Half Of 2024

Emerging Threats & Vulnerabilities

- PythonAnywhere Cloud Platform Abused for Hosting Ransomware
- Critical flaw in WPML WordPress plugin impacts 1M websites
- South Korean Spies Exploit WPS Office Zero-Day
- Malware Infiltrates Pidgin Messenger's Official Plugin Repository
- Microsoft Fixes ASCII Smuggling Flaw That Enabled Data Theft from Microsoft 365 Copilot

Attacks, Breaches, & Leaks

- U.S. Marshals Service Disputes Ransomware Gang's Breach Claims
- 2 TB of Sensitive "ServiceBridge" Records Exposed in Cloud Misconfiguration
- Young Consulting Data Breach Impacts 954,177 Individuals
- Data Breach Hits Fans of 26 Baseball Teams in Minnesota, Wisconsin, Iowa + 4 More States

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

EXECUTIVE NEWS

City Of Columbus Tries To Silence Security Researcher
Malwarebytes, 9/3/2024

The City of Columbus, Ohio is suing a security researcher for sharing stolen data. All the complaint will accomplish, we imagine, is spotlight the ignorance of certain city officials in handling a common security matter. What happened is that the City of Columbus was attacked by a ransomware group on July 18, 2024. Due to the timing, it was at first unclear whether the disruption in the public facing services was caused by the CrowdStrike incident or if it was in fact an attack. The attack was later claimed by the Rhysida ransomware group on their leak site, where the group posts information about recent victims that are unwilling to pay. https://www.malwarebytes.com/blog/news/2024/09/city-of-columbus-tries-to-silence-security-researcher

Iranian-Linked Hackers Collaborate With Ransomware Affiliates, Feds Say
Cyber Scoop, 8/28/2024

Iranian-sponsored hackers are acting as access brokers for ransomware affiliates like ALPHV, U.S. intelligence agencies warned in a joint alert Wednesday. The FBI, Cybersecurity and Infrastructure Security Agency, and the Department of Defense's Cyber Crime Center said in an advisory that hackers with likely sponsorship from Iran are moonlighting with notable ransomware affiliates and seeking out network access to organizations in education, finance, health care, and defense. Those groups will then collaborate with the affiliates to help deploy ransomware for a cut of the extortion, the alert said. The joint advisory is the latest Iranian-backed operation highlighted by cybersecurity firms and intelligence agencies, following a slew of reports within the past few weeks. https://cyberscoop.com/iran-cisa-fbi-ransomware-advisory/

Censys Finds Hundreds of Exposed Servers as Volt Typhoon APT Targets Service Providers
Security Week, 8/28/2024

Censys shared live search queries Wednesday showing hundreds of exposed Versa Director servers pinging from the US, Philippines, Shanghai and India and urged organizations to isolate these devices from the internet immediately. It is not quite clear how many of those exposed devices are unpatched or failed to implement system hardening guidelines (Versa says firewall misconfigurations are to blame) but because these servers are typically used by ISPs and MSPs, the scale of the exposure is considered enormous. Even more worrisome, more than 24 hours after disclosure of the zero-day, anti-malware products are very slow to provide detections for VersaTest.png, the custom VersaMem web shell being used in the Volt Typhoon attacks. https://www.securityweek.com/censys-finds-hundreds-of-exposed-servers-as-volt-typhoon-apt-targets-isps-msps/

Researchers Find SQL Injection To Bypass Airport TSA Security Checks
Bleeping Computer, 8/30/2024

Security researchers have found a vulnerability in a key air transport security system that allowed unauthorized individuals to potentially bypass airport security screenings and gain access to aircraft cockpits. Researchers Ian Carroll and Sam Curry discovered the vulnerability in FlyCASS, a third-party web-based service that some airlines use to manage the Known Crewmember (KCM) program and the Cockpit Access Security System (CASS). KCM is a Transportation Security Administration (TSA) initiative that allows pilots and flight attendants to skip security screening, and CASS enables authorized pilots to use jumpseats in cockpits when traveling. https://www.bleepingcomputer.com/news/security/researchers-find-sql-injection-to-bypass-airport-tsa-security-checks/

Hitachi Energy Vulnerabilities Plague SCADA Power Systems
Dark Reading, 8/28/2024

Hitachi Energy is urging customers of its MicroSCADA X SYS600 product for monitoring and controlling utility power systems to immediately upgrade to a newly released version to mitigate multiple critical and high-severity vulnerabilities. In a security advisory this week, the company described the vulnerabilities as enabling attacks that could have serious confidentiality, integrity, and availability impacts on affected products. Hiatchi's MicroSCADA X SYS600 is a system that it acquired from its purchase of ABB's Power Grids business. Hitachi Electric says the technology is currently deployed across more than 10,000 substations, and is being used to manage and monitor power across power grids, process industries, data centers, seaports, hospitals, railways, and at least 30 airports.
https://www.darkreading.com/ics-ot-security/hitachi-energy-vulnerabilities-plague-scada-power-systems

Published Vulnerabilities Surge by 43%
HelpNet Security, 8/27/2024

Published vulnerabilities rose by 43% in H1 2024 compared to H1 2023, with attackers heavily targeting flaws in virtual private networks (VPNs) and other perimeter devices for initial access, a new report from Forescout has found. The majority of published vulnerabilities in H1 2024 had either a medium (39%) or low (25%) severity score (CVSS), while just 9% had a critical score. This is in contrast to the same period last year, where around two-thirds of vulnerabilities were either medium (39%) or high (27%). The report also highlighted that 87 CVEs were added to the US Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) catalog in H1 2024, bringing the total to 1140 vulnerabilities. This represents a decrease of 23% compared to the same period in 2023.
https://www.infosecurity-magazine.com/news/published-vulnerabilities-surge/

Cyber Threats That Shaped The First Half Of 2024
Help Net Security , 8/30/2024

Global cybercrime has shown no sign of decline and is expected to grow strong per year over the next five years. To identify the most urgent cybersecurity threats of the first half of 2024, the Critical Start Cyber Research Unit (CRU) analyzed 3,438 high and critical alerts generated by 20 supported EDR solutions, as well as 4,602 reports detailing ransomware and database leak activities across 24 industries in 126 countries. The first half of 2024 saw a worrying trend in cyberattacks targeting specific industries and key report findings include: Manufacturing and Industrial Products remains the top targeted industry by cyber threat actors in H1 2024, leading with 377 confirmed reports of ransomware and database leak hits in the first half of the year. https://www.helpnetsecurity.com/2024/08/30/cyber-threat-intelligence-report-key-threats/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TECHNICAL SUMMARY

EMERGING THREATS & EXPLOITS

- ***PythonAnywhere Cloud Platform Abused for Hosting Ransomware*** – Razr ransomware is exploiting PythonAnywhere to distribute and encrypt files with AES-256. ANY.RUN's analysis reveals its behaviour, C2 communication, and ransom demands via Tor. Protect your systems with ANY.RUN's free malware analysis tools and stay ahead of this threat. https://hackread.com/pythonanywhere-cloud-platform-abused-for-hosting-ransomware/
- ***Critical flaw in WPML WordPress plugin impacts 1M websites*** **-** A critical flaw in the WPML WordPress plugin, which is installed on 1 million websites, could allow potential compromise of affected sites. https://securityaffairs.com/167673/hacking/wpml-wordpress-plugin-rce-1m-websites.html
- ***South Korean Spies Exploit WPS Office Zero-Day*** **-** ESET has revealed a new cyber-espionage campaign linked to a South Korean APT in which a novel remote code execution (RCE) vulnerability in WPS Office for Windows was exploited to deploy a custom backdoor. https://www.infosecurity-magazine.com/news/south-korean-spies-exploit-wps/
- ***Malware Infiltrates Pidgin Messenger's Official Plugin Repository*** **-** The Pidgin messaging app removed the ScreenShareOTR plugin from its official third-party plugin list after it was discovered that it was used to install keyloggers, information stealers, and malware commonly used to gain initial access to corporate networks. https://www.bleepingcomputer.com/news/security/malware-infiltrates-pidgin-messengers-official-plugin-repository/
- ***Microsoft Fixes ASCII Smuggling Flaw That Enabled Data Theft from Microsoft 365 Copilot*** **-** Details have emerged about a now-patched vulnerability in Microsoft 365 Copilot that could enable the theft of sensitive user information using a technique called ASCII smuggling. https://thehackernews.com/2024/08/microsoft-fixes-ascii-smuggling-flaw.html

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ATTACKS, BREACHES & LEAKS

- ***U.S. Marshals Service Disputes Ransomware Gang's Breach Claims*** – The U.S. Marshals Service (USMS) denies its systems were breached by the Hunters International ransomware gang after being listed as a new victim on the cybercrime group's leak site on Monday. https://www.bleepingcomputer.com/news/security/us-marshals-service-disputes-ransomware-gangs-breach-claims/
- ***2 TB of Sensitive "ServiceBridge" Records Exposed in Cloud Misconfiguration*** **-** A major database misconfiguration exposed millions of sensitive records belonging to ServiceBridge customers. Learn about the risks and consequences of this data exposure and how businesses can protect themselves from similar incidents. https://hackread.com/servicebridge-expose-2tb-records-cloud-misconfiguration/
- ***Young Consulting Data Breach Impacts 954,177 Individuals*** **-** A ransomware attack by the BlackSuit group on Young Consulting compromised the personal information of over 950,000 individuals. https://securityaffairs.com/167714/data-breach/blacksuit-group-attack-young-consulting.html
- ***Data Breach Hits Fans of 26 Baseball Teams in Minnesota, Wisconsin, Iowa + 4 More States*** **-** Fans who attended a Northwoods League baseball or softball game across Minnesota, Wisconsin, Iowa, North Dakota, Illinois, Michigan, and Indiana this past summer may have had their personal information compromised in a recent data breach, according to a notification from the Northwoods League, Inc. The breach, which was discovered on July 17, 2024, involved the league's online ticketing system, impacting teams and event managers across the league. https://krocnews.com/northwoods-baseball-league-data-breach/?utm_source=tsmclip&utm_medium=referral

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

SECURITY VULNERABILITIES, ALERTS, ADVISORIES, & UPDATES

SUSE Security Updates

1. Rsyslog - https://www.suse.com/support/update/announcement/2024/suse-ru-20243135-1
2. perl-DBI - https://www.suse.com/support/update/announcement/2024/suse-su-20243136-1
3. mozilla-nss - https://www.suse.com/support/update/announcement/2024/suse-ru-20243137-1
4. crmsh - https://www.suse.com/support/update/announcement/2024/suse-ru-20243138-1
5. python-Django - https://www.suse.com/support/update/announcement/2024/suse-su-20243139-1
6. java-1_8_0-openj9 - https://www.suse.com/support/update/announcement/2024/suse-su-20243140-1
7. python-kiwi - https://www.suse.com/support/update/announcement/2024/suse-ru-20243141-1
8. cargo-auditable - https://www.suse.com/support/update/announcement/2024/suse-ru-20243142-1
9. sles-release - https://www.suse.com/support/update/announcement/2024/suse-ru-20243143-1

Fedora Security Advisories

1. seamonkey - https://lwn.net/Articles/988712
2. apr - https://lwn.net/Articles/988711

Mageia Security Advisories

1. php - http://advisories.mageia.org/MGAA-2024-0190.html

Slackware Linux Security Advisories

1. mozilla-firefox - http://www.slackware.com/security/viewer.php?l=slackware-security&y=2024&m=slackware-security.377367
2. seamonkey - http://www.slackware.com/security/viewer.php?l=slackware-security&y=2024&m=slackware-security.346366

Red Hat Security Advisories

1. OpenShift - https://access.redhat.com/errata/RHSA-2024:6274

OTHER

1. Chrome Beta Desktop - https://chromereleases.googleblog.com/2024/09/chrome-beta-for-desktop-update.html
2. Chrome Beta Android - https://chromereleases.googleblog.com/2024/09/chrome-beta-for-android-update.html