Cyber Brief (September 2024)

October 1, 2024 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 269 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, in Europe, law enforcement agencies dismantled infrastructure of at least five distinct cybercrime actors, a former Polish Minister of Justice was charged with unlawfully purchasing Pegasus spyware, and Ukraine banned Telegram on governmental and critical infrastructure. Elsewhere, the Turkish National Intelligence Organisation dismantled a cyberespionage network that had reportedly shared information with terrorist organisations, while the US announced a proposed ban on Chinese and Russian Vehicle Connected System IT, sanctioned five individuals and one entity linked to the Intellexa Consortium for their role in developing and distributing Predator spyware, and took several steps to secure its upcoming Presidential elections.
- On the **cyberespionage** front, in Europe, Chinese intelligence targeted Czech researchers with LinkedIn spearphishing, and APT28 allegedly targeted German Air Traffic Control systems. Elsewhere, the US government reported that China-linked Salt Typhoon intruded multiple US telecommunication entities, while UNC1860, an Iranian state-sponsored threat actor likely affiliated with MOIS (Ministry of Intelligence of the Islamic Republic of Iran), targeted Middle Eastern networks, targeting telecommunications and government sectors and Predator spyware resurged in Congo and Angola.
- Relating to **cybercrime**, in Europe, Transport for London disclosed that it experienced a cyberattack, and unidentified cybercrime actors targeted French users with AI-generated malware. Elsewhere, North Korea-linked Citrine Sleet exploited a Chromium zero-day to target the cryptocurrency sector for financial gain and a water treatment facility in the US resorted to manual operations following a ransomware attack.
- Relating to **destructive** attacks, a multinational joint technical advisory exposed destructive threat actor Cadet Blizzard, responsible for Whispergate attacks in Ukraine, as being connected to Russian GRU Unit 29155.
- As regards **data exposure and leaks** incidents, the Dutch National Police experienced a data breach, while a BreachForums account claimed a hack-and-leak of Dell employee data.

- On the **hacktivism** front, pro-Russia supposed hacktivists continued their long-running campaign of DDoS attacks on strategic moments, this month, NoName057(16) conducted a DDoS attack on the websites of Austrian entities ahead of their Parliamentary elections.
- Relating to **information operations**, the Swedish government called out the Iranian Islamic Revolutionary Guard Corps (IRGC) for an influence campaign which involved sending bulk text messages to Swedes.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in September 2024.

Europe

Cyber policy and law enforcement

Ukraine bans Telegram App on governmental and military infrastructure
On September 19, the Ukrainian National Coordination Centre for Cybersecurity (NCCC), a key body for coordination and control in the field of cybersecurity, decided to restrict the use of Telegram in government agencies, military formations, and critical infrastructure facilities. The NCCC considers the App a threat to Ukrainian national security because Telegram is actively used by the enemy for cyberattacks, spreading phishing and malware, establishing the geolocation of users and adjusting missile strikes. `ban` `russia` `ukraine war`

Former Polish Minister of Justice charged with purchasing Pegasus Spyware
On August 27, a former Polish Deputy Minister of Justice was charged with exceeding his authority and failing to fulfill his duties by transferring PLN 25 million from the Justice Fund to the Central Anticorruption Bureau between September and November 2017 for the purchase of Pegasus software, violating legal funding restrictions. He faces up to 10 years in prison. Preventive measures, including police supervision, have been applied. `psoa`

Polish government plans to update electronic communication regulations following Russian and Belarusian attacks
On September 9, the Polish Minister of Interior announced that following several cyberattacks from an unnamed Russian and Belarusian threat actor in 2024 the government was updating electronic communication regulations. Targets included the Polish Anti-Doping Agency, Polish Press Agency, local government, and state companies connected to national security. In August an unspecified attack was foiled which was intended to cause political, military and business paralysis of the Polish state. `public administration` `russia`

Europol dismantles iServer phishing as a service platform
On September 19, Europol announced it dismantled an international cybercrime network. The network managed a Phishing-as-a-Service (PaaS) platform with over 483,000 predominantly Spanish-speaking victims. Law enforcement estimates that the threat actors used the iServer PaaS platform to target over one million phones via phishing. `takedown`

Europol dismantles criminal network responsible of unlocking stolen phones of 483,000 victims
On September 19, Europol announced the dismantle of an international criminal network responsible for unlocking stolen and lost mobile phones through the iServer phishing-as-a-service platform. Operation Kaerb, initiated in 2022 by Europol and involving multiple countries, identified 483,000 victims. Law enforcement arrested 17 suspects, including the platform's Argentinian administrator, and seized 921 items. Over 2,000 criminals used iServer to steal credentials, targeting over 1.2 million devices globally. `arrest`

German police seizes the data leak site of Vanir Ransomware Group

On September 17, German police officials announced the seizure of the Vanir Ransomware Group data leak site (DLS). According to the DLS, Vanir Ransomware Group posted their first victim on June 3, 2024 and their last on July 7. `seizure`

German Federal Police Office takes down 47 money laundering services in Germany

On September 19, the Federal Criminal Police Office and the Central Office for Combating Cybercrime took down 47 Germany-hosted exchange services used for money laundering. These platforms facilitated anonymous cryptocurrency exchanges without implementing Know-Your-Customer protocols, aiding ransomware groups, darknet traders, and botnet operators in laundering illicit funds. The operation secured extensive user and transaction data for further investigations into cybercrime.

Europol dismantles Ghost encrypted messaging platform used for organised crime

On September 18, Europol and nine countries dismantled the Ghost encrypted communications platform, used for organised crime such as drug trafficking and money laundering. Ghost featured advanced encryption, self-destructing messages, and cryptocurrency payments. The investigation led to the arrest of 51 individuals, seizure of EUR 1 million, and the dismantling of a drug lab. Authorities highlighted the ongoing challenge of monitoring fragmented encrypted communication platforms used by criminals. `seizure`

Cyberespionage

Chinese intelligence targets Czech researchers with LinkedIn spearphishing campaign

On September 12, Czechia's Security Information Service (BIS) reported that China-nexus intelligence targeted Czech researchers via LinkedIn throughout 2023, posing as recruiters or consultants from Singapore or Hong Kong. The attackers requested sensitive reports and offered financial rewards, aiming to gather intelligence and disseminate propaganda. BIS also noted a decline in spearphishing targeting Czech government agencies by China-nexus groups. `china`

Cyberattack targets German Air Traffic Control systems

On September 1, Der Spiegel reported about a cyberattack targeting the German Air Traffic Control's administrative IT systems with alleged links to APT28. Air traffic safety remained unaffected. German security agencies, including the Federal Office for Information Security (BSI), are investigating the incident. No data breach has been confirmed. `russia`

Cybercrime

Unknown cybercrime actors target French users with AI-generated malware

On September 24, HP threat researchers reported on their discovery of a malware campaign targeting French users. The attack used AI-generated code to deliver AsyncRAT via HTML smuggling. The VBScript loader features detailed and systematic comments, suggesting AI involvement. Once executed, it created scheduled tasks, modified the Windows Registry, and executed AsyncRAT for remote access and control. `artificial intelligence`

Transport for London discloses incident

On September 3, Transport for London (TfL) announced it was investigating a cyberattack with no impact on services or evidence of compromised customer data. TfL has reported the incident to government agencies and implemented measures to secure its systems. Previously, in July, TfL confirmed that the Cl0p ransomware gang breached a supplier's server, affecting 13.000 customer contact details. `transport`

Destructive

Joint technical advisory exposes Russian Cadet Blizzard
On September 5, Latvia, the Netherlands, Estonia , Germany, Czechia, the US, and several other countries issued a joint statement attributing Cadet Blizzard (Ember Bear) to Russian GRU Unit 29155. They detailed Cadet Blizzard's WhisperGate attack techniques and revealed infrastructure used by the group. `destructive` `russia`

Information operations

Sweden calls out IRGC for influence campaign involving bulk text messages to Swedes
On September 25, the Swedish Security Service reported that in 2023, an Iranian cyber group acted on assignment by the Iranian Islamic Revolutionary Guard Corps (IRGC) to carry out an influence campaign in Sweden. The group intruded a company that has a bulk text messaging service and sent out a huge number of text messages to Swedes urging acts of revenge against Quran burners, in an effort to portray Sweden as anti-Islam and to create divisions. `iran`

Data exposure and leaks

Incident involving The Netherlands' National Police leads to data breach
On September 26, the Netherlands' National Police disclosed that an unnamed threat actor compromised a police officer's account, resulting in the theft of work-related contact details of police employees. No investigative data was exposed.

Incident affecting Agence France Presse
On September 28, the Agence France Presse (AFP) publicly announced that they suffered a cybersecurity incident. This incident involves the compromise of a specific device related to their Information delivery system (FTP/SFTP server). AFP took action to stop the incident shortly after discovering the incident and notified clients.

Hacktivism

NoName057(16) DDoS websites of Austrian entities ahead of their Parliamentary elections
On September 26, NoName057(16), a pro-Russia supposed hacktivist, claimed DDoS attacks against Austrian public and private sector entities' websites. The claims were tied to Austria's legislative elections on 29 September. `election` `public administration` `russia`

World

Cyber policy and law enforcement

US announces proposed ban on Chinese and Russian Vehicle Connected System IT
On September 26, the US Department of Commerce published a notice on a proposed rule to prohibit transactions involving Vehicle Connectivity System hardware and covered software designed, developed, manufactured, or supplied by people controlled by the jurisdiction of China, including Hong Kong, or Russia. `automotive` `china` `russia` `technology` `transport` `united states` `ban`

Tor Project and Tails merge to strengthen digital privacy and security
On September 26, the Tor Project and Tails merged to enhance collaboration, sustainability, and outreach in the fight against global surveillance and censorship. Tails, a secure operating system, will benefit from the Tor Project's resources, allowing it to focus on improving digital security tools. This merger will increase training opportunities and provide stronger protections for high-risk users, such as journalists and activists, combining Tor's network security with Tails' system-level defences. `privacy`

US sanctions individuals linked to Intellexa to counter spyware proliferation
On September 16, the Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned five individuals and one entity linked to the Intellexa Consortium for their role in developing and distributing Predator spyware, deemed as a significant threat to US national security. The sanctions target those responsible for commercial spyware misuse, part of broader US efforts to counter spyware proliferation through sanctions, export controls, and visa restrictions. `psoa` `united states`

Meta bans RT and Russian state media over foreign interference
Meta has banned RT and other Russian state media from its platforms globally, citing their involvement in foreign interference. The ban applies to Facebook, Instagram, WhatsApp, and Threads, and comes after the Biden administration imposed sanctions on these outlets. RT criticised the decision, claiming it would continue to bypass restrictions. The US has labeled RT as part of Moscow's intelligence apparatus. `social media and messaging` `ban`

Turkey to propose a standalone cybersecurity agency amid regional tensions
On September 19, Anadolu Agency, Turkey's state-run news service, reported that Foreign Minister announced plans to propose a standalone cybersecurity agency. The proposal aligns with Turkey's updated National Cybersecurity Strategy and Action Plan (2024-2028). `turkey`

Kaspersky to be replaced with UltraAV in the US
On September 23, Bleeping Computer reported that Kaspersky emailed US customers to report that they would receive cybersecurity protection from UltraAV after Kaspersky stopped selling software. Reportedly, as from September 26, Kaspersky plans to delete its anti-malware software from US customers' computers and automatically replace it with UltraAV's antivirus solution. These developments follow the June US government decision to deem Kaspersky a national security concern and ban its sale in the US. `united states` `ban`

Telegram to start sharing phone numbers and IP addresses with law enforcement in certain cases
On September 23, Telegram updated its privacy policy to include that Telegram will comply with law enforcement requests to provide IP addresses and phone numbers of users only after receiving a valid court order. The court order needs to confirm that the user is a suspect in a criminal case that breaches the platform's Terms of Service. `world`

FBI disrupts China-linked Raptor Train botnet compromising over 200,000 IoT devices since 2020
On 18 September, the US Department of Justice announced the disruption of a botnet of over 200,000 devices controlled by Chinese state-sponsored hackers from Integrity Technology Group. The botnet, linked to hackers known as Flax Typhoon, infected consumer devices globally. The FBI led the operation, issuing malware-disabling commands and fending off a DDoS attack. `china` `takedown`

Turkish National Intelligence Organisation dismantles global cyberespionage network
On August 27, the Turkish National Intelligence Organisation (MIT) dismantled a global cyberespionage network that had reportedly stolen and shared personal data, including with terrorist organisations. Eleven suspects were arrested, and associated websites were shut down.

MIT plans to expand its operations to protect sensitive data and address international cyber threats, reinforcing national security efforts. `cyberespionage` `arrest`

US indicts Russian state media and US company in 2024 election interference scheme
On September 4, the US Department of Justice indicted two Russian state media employees and two unnamed founders of a Tennessee-based company for conspiracy related to a covert Russian influence operation targeting US audiences ahead of the 2024 election. The indictment reveals that the Russian government used this company to promote pro-Russian content through US media channels, part of a broader effort to influence American political discourse. `election` `indictment` `russia` `united states`

US identifies FSB officer who set up pro-Russia supposed hacktivist group RaHDit
On September 4, the US government took actions against RaHDit, a pro-Russia supposed hacktivist, for acting on behalf of Russia's Federal Security Service (FSB) as well as for supporting cyber-enabled election interference and Russian state disinformation. The US government announced a reward 10 million US dollars for information about RaHDit, and identified a former FSB officer who allegedly established RaHDit while working at the FSB. `election` `russia` `united states`

US targets Russian disinformation network ahead of elections
On September 4, the US government announced the FBIs seizure of 32 domains used by the Russian-linked Doppelgänger disinformation network. The group, tied to Russian companies, spread propaganda to influence the 2024 US election. Using typosquatting, AI-generated content, and fake profiles, they misled viewers, promoting pro-Russia narratives. They also indicted two Russian nationals involved in distributing pro-Russia disinformation. `russia` `united states` `indictment` `seizure`

Chinese national indicted for spearphishing US military and aerospace organisations
On September 16, the US Department of Justice indicted Song Wu, a Chinese national, for spearphishing US military and aerospace organisations to steal proprietary aerospace source code and software. Employed by Aviation Industry Corporation of China (AVIC), Wu impersonated colleagues to target engineers and researchers from 2017 to 2021. `united states` `indictment`

Cyberespionage

Suspected China-linked actor Earth Baxia exploits GeoServer vulnerability
On September 19, Trend Micro reported about Earth Baxia, a threat actor likely based in China, targeting government organisations in Taiwan and other APAC countries through exploiting GeoServer vulnerability CVE-2024-36401. Their campaign leveraged public cloud services for hosting malicious files, targeting the government, telecommunications, and energy sectors across APAC. We have previously observed an unattributed global campaign also exploiting CVE-2024-36401 to deliver cryptominers. `china` `energy` `public administration` `telecommunications`

China-linked Salt Typhoon intrudes multiple US telecommunication entities
On September 26, The Wall Street Journal reported that Salt Typhoon, a China-linked threat actor intruded multiple US telecommunication entities in recent months. Salt Typhoon reportedly gained access to sensitive information and established persistence, which allegedly could be used in future conflict scenarios. `china` `prepositioning` `telecommunications` `united states`

Chinese made cranes pose cybersecurity risk to US port infrastructure
A September 2024 US congressional investigation revealed that China-manufactured ship-to-

shore cranes used in US ports, produced by Shanghai Zhenhua Heavy Industry (ZPMC), have embedded cellular modems. These modems could allow Chinese intelligence to access US data and control systems. ZPMC's compliance with China's cybersecurity laws likely facilitates governmental access to source codes, posing a significant cybersecurity risk to US port infrastructure. `china` `supply-chain attack` `united states`

China-linked Flax Typhoon targets entities in Taiwan and South Korea using SoftEther VPN software

On September 19, a trusted partner reported about Flax Typhoon continuing to target networks in Taiwan and South Korea using SoftEther VPN software. Flax Typhoon compromised web servers of two Taiwan-based technology companies. They maintained access via MeshCentral software and compromised networks in South Korea, India, Kenya, Rwanda, and Nigeria. The group used an ORB network of likely compromised SOHO devices for unclear purposes, focusing on Asia and Africa. `china` `technology`

India-linked threat actpr SloppyLemming espionage campaign against South and East Asia

On September 24, Cloudflare security researchers reported on the India-linked threat actor SloppyLemming targeting South and East Asian countries, focusing on governments, defence, and technology sectors. Using open-source tools like Cobalt Strike, the group conducts phishing attacks for credential harvesting, primarily in Pakistan, Bangladesh, and China. `china` `defence` `india` `public administration` `technology`

Credential phishing campaign mimics legitimate webmail login portals targeting South Asia and China

On September 18, NetmanageIT reported that, since August 2024, an India-nexus intrusion actor has been targeting government and defence entities in China and South Asia using credential phishing pages that imitate legitimate webmail portals. The phishing pages are hosted on domains registered via 1api with Royalhost name servers. The domain naming conventions and tactics used suggest the activity is linked to Indian targeted intrusion groups, such as Sidewinder and Patchwork. `china` `india`

Mandiant assesses UNC1860 to specialise in sophisticated initial access and persistence operations for Iran's MOIS

On September 19, Mandiant reported on UNC1860, an Iranian state-sponsored threat actor likely affiliated with MOIS. UNC1860 uses specialised tools and passive backdoors to gain persistent access to high-priority Middle Eastern networks, targeting telecommunications and government sectors. Tools like Templeplay and Virgeen enable remote access and facilitate collaboration with other threat actors. UNC1860's tactics align with other Iran-based groups, demonstrating reverse engineering capabilities and a focus on espionage and network attack operations in the region. `iran` `public administration` `telecommunications`

North Korea-linked UNC2970 deploys backdoor using trojanised PDF reader to target critical infrastructure

On September 17, Mandiant reported that cyberespionage group UNC2970, suspected of North Korean ties, targeted US critical infrastructure by distributing phishing lures disguised as job offers. The phishing campaigns primarily targeted senior employees in energy and aerospace sectors, aiming to steal sensitive information through the modified job descriptions. `aerospace` `energy` `north korea` `united states`

Resurgence of Predator spyware likely targeting high-profile individuals in multiple countries

On September 5, Recorded Future security researchers reported on the resurgence of Predator spyware infrastructure. Despite sanctions and media exposure, threat actors resumed operations, now using enhanced evasion tactics. New infrastructure was detected in multiple countries, including the Democratic Republic of the Congo and Angola, continuing to target high-profile individuals. `psoa`

Cybercrime

North Korea-linked Citrine Sleet exploited Chromium zero-day

On August 30, Microsoft reported with medium confidence that Citrine Sleet, a North Korean threat actor, exploited a Chromium zero-day vulnerability on August 19 to perform remote code execution. The Chromium vulnerability was identified as CVE-2024-7971 and fixed on August 21. Microsoft assesses that Citrine Sleet used the Chromium zero-day to target the cryptocurrency sector for financial gain.

Threat actors exploit authentication misconfiguration in Selenium Grid for cryptomining and proxyjacking

On September 17, Cado Security identified two campaigns exploiting misconfigured Selenium Grid instances for cryptomining and proxyjacking. Threat actors leveraged the lack of authentication to deploy malicious scripts, including cryptominers like “perfcc” and proxyjacking tools. The attacks involved injecting Python scripts via Selenium Grid configurations, executing reverse shells, and installing payloads such as IPRoyal and Traffmonetizer. The campaigns highlight the risk of misconfigured Selenium Grid setups, urging the need for authentication.

Scam campaigns using deepfake AI-generated videos

On August 29, Palo Alto Networks reported about deepfake scam campaigns using AI-generated videos of public figures, such as CEOs and politicians, to promote fraudulent investment schemes and government giveaways. These scams target various countries and appear in multiple languages. The infrastructure analysis suggests these campaigns likely originate from a single threat actor group, using hundreds of domains and shared hosting networks to avoid detection. `artificial intelligence`

Water treatment facility in Arkansas City resorts to manual operations following ransomware attack

On September 23, the Arkansas City (US) water treatment facility reported that it had suffered a ransomware attack which had led them to revert to manual operations. The incident began on September 22 and reportedly included an unspecified ransom demand. `critical infrastructure` `united states`

Scattered Spider targets insurance and financial sectors with cloud-based ransomware attacks

On September 10, Eclecticiq reported that Scattered Spider (Storm-0875), a cybercriminal group, has been actively targeting cloud infrastructures such as AWS, Entra ID and GCP, in the insurance and financial sectors using social engineering techniques like vishing and smishing to gain unauthorised access. The group leverages cloud-native tools and SIM-swapping techniques to bypass multi-factor authentication, exfiltrate sensitive data, and deploy ransomware, making detection and defence challenging. `finance` `insurance`

Data exposure and leaks

BreachForums account claims hack-and-leak of Dell employee data

On September 20, Bleeping Computer reported that Dell, a US technology company, confirmed to them that they are investigating a recent reported hack-and-leak involving the data for over 10,000 Dell employees. On September 19, Grep, an account active on BreachForums, alleged that Dell suffered a data breach in September 2024, allegedly exposing internal employee and partner information. `technology`

Information operations

Russia and Iran target 2024 US election with influence campaigns
On September 18, Microsoft reported that Russia and Iran are conducting influence operations targeting the 2024 US election. Russia shifted its focus from President Biden to Vice President Harris, utilizing cyber proxies and hacktivist groups like Ruza Flood and RaHDit. The campaign involves spreading disinformation, AI-enhanced propaganda, and divisive content. Iran is also expected to continue its influence efforts targeting Republican campaigns. Both nations aim to disrupt voter trust and election security. `election` `iran` `russia` `united states`

Iran's information operations targeting upcoming US elections
On September 4, the New York Times reported on Iran's increased disinformation efforts aimed at influencing the US presidential election, using fake websites and social media. These campaigns target both Donald Trump and the overall US electoral system, aiming to sow discord and distrust. US officials and analysts note that Iran's tactics have become more aggressive, similar to influence operations by other nations, including Russia and China. `election` `iran` `united states`

Ukraine dismantles two bot farms linked to Russian disinformation campaigns
On September 3, the Security Service of Ukraine reported shutting down two bot farms linked to Russian disinformation campaigns. One operator created nearly 15.000 accounts on different social media platforms on behalf of the Russian Intelligence Service while the other operator sold unique IP addresses to Russian users, allowing them to impersonate Ukrainians online. `russia`

Hacktivism

Pro-Russia hacktivists launch DDoS attacks against Taiwan over China-Russia relations statements
On September 9, pro-Russia hacktivist groups, led by NoName057 and the Cyber Army of Russia, launched a DDoS campaign against Taiwanese public and private entities in retaliation for statements made by Taiwanese President Lai Ching Te about China-Russia relations. The attack reflects these group's responsiveness to geopolitical events perceived as harmful to Russian interests and represents a shift in their typical focus on Europe-based targets. `china` `russia`

Pro-Israel hacktivist group claims control of Hezbollah water systems
On September 26, the pro-Israel hacktivist group Red Evil claimed to have hacked SCADA systems controlling 14 water facilities used by Hezbollah in Lebanon, altering chlorine levels to cause harm. The US cybersecurity agency CISA warned that even unsophisticated methods can be used to hack industrial systems, though some claims by threat actors may be exaggerated. `industrial control system (ics)` `israel`

Significant vulnerabilities

Multiple Vulnerabilities in Cisco NX-OS Software On August 28, Cisco released patches for multiple vulnerabilities affecting its NX-OS software, primarily used in Nexus switches. The most severe of these is a high-severity denial-of-service (DoS) vulnerability in the DHCPv6 relay agent, which could allow an unauthenticated remote attacker to cause targeted devices to reload repeatedly, leading to a DoS condition. Additionally, several medium-severity vulnerabilities were addressed, including issues that could allow privilege escalation and unauthorised code execution. See CERT-EU's SA 2024-090.

High Severity Vulnerability in VMware Fusion for MacOS On September 3, Broadcom disclosed a high-severity vulnerability in VMware Fusion, which could allow attackers to execute arbitrary code on macOS systems. See CERT-EU's SA 2024-091.

Critical Vulnerability in Veeam On September 5, Veeam disclosed a critical remote code execution (RCE) vulnerability tracked as CVE-2024-40711, affecting Veeam Backup & Replication (VBR). This flaw allows unauthenticated attackers to execute arbitrary code on vulnerable systems (CVSS score: 9.8). VBR is a target for ransomware attacks, as it plays a key role in enterprise data protection. Users are advised to update to version 12.2.0.334 as soon as possible. See CERT-EU's SA 2024-092.

Multiple Critical Vulnerabilities in Microsoft Products On September 10, Microsoft addressed 79 vulnerabilities in its September 2024 Patch Tuesday update, including four zero-day vulnerabilities. This Patch Tuesday also fixes seven critical vulnerabilities. See CERT-EU's SA 2024-093.

Critical Vulnerabilities in Ivanti EPM On September 10, Ivanti addressed several critical and high security vulnerabilities its Endpoint Manager (EPM) product. It is recommended updating as soon as possible. See CERT-EU's SA 2024-094.

Critical vulnerabilities in Adobe Products On September 10, Adobe released a security bulletin addressing two critical vulnerabilities affecting its Acrobat products. When exploited, these vulnerabilities could allow an attacker to execute arbitrary code. A publicly available proof-of-concept exploit exists for one of the vulnerabilities. See CERT-EU's SA 2024-095.

Vulnerabilities in GitLab On September 11, GitLab released a security advisory addressing several vulnerabilities, one of which being critical, allowing an attacker to trigger pipelines as arbitrary users under certain conditions. See CERT-EU's SA 2024-096.

Vulnerabilities in SolarWinds Access Rights Manager On September 12, Solarwinds released several advisories addressing two critical vulnerabilities in SolarWinds Access Rights Manager (ARM). These vulnerabilities, if exploited, could lead to authenticated remote code execution, and authentication bypass. See CERT-EU's SA 2024-097.

Command Injection Vulnerability in PaloAlto PAN-OS On September 11, a high-severity command injection vulnerability has been addressed in PaloAlto PAN-OS. If exploited, this flaw could allow an authenticated attacker to execute arbitrary commands as root on the firewall. See CERT-EU's SA 2024-098.

Critical Vulnerabilities in Openshift On 16th of September 2024, two vulnerabilities (CVE-2024-45496 and CVE-2024-7387) have been discovered in Red Hat systems that allow attackers to escalate privileges or execute arbitrary code, impacting system integrity. See CERT-EU's SA 2024-099.

Critical RCE Vulnerability in VMware vCenter Server On September 17, Broadcom released a fix for a critical vulnerability tracked as CVE-2024-38812 in VMware vCenter Server, enabling remote code execution (RCE) via a specially crafted network packet. See CERT-EU's SA 2024-100.

Critical SAML Authentication Bypass in Gitlab On September 17, GitLab issued a security advisory addressing a critical vulnerability identified in GitLab's SAML authentication implementation, potentially allowing attackers to bypass authentication. The vulnerability affects the Community Edition (CE) and the Enterprise Edition (EE) instances that utilise SAML for single sign-on (SSO). See CERT-EU's SA 2024-101.

Traefik Critical Vulnerability On September 19, a security advisory was issued regarding a critical vulnerability, CVE-2024-45410, affecting Traefik. This vulnerability could allow an attacker to

execute arbitrary commands via crafted HTTP requests, posing a significant risk to exposed services. See CERT-EU's SA 2024-102.

Critical Vulnerabilities in CUPS On September 26, a security researched released a blog post describing several vulnerabilities in CUPS, one of which being critical, allowing an attacker to replace existing printers' IPP URLs with a malicious one, resulting in a potential arbitrary command execution. See CERT-EU's SA 2024-103.

Critical Vulnerability in NVIDIA Container Toolkit On September 26, a security advisory was issued regarding a critical vulnerability, CVE-2024-0132, affecting NVIDIA Container Toolkit. NVIDIA Container Toolkit is providing containerised AI applications with access to GPU resources. This vulnerability impacts any AI application that is running the vulnerable container toolkit to enable GPU support. See CERT-EU's SA 2024-104.

Multiple Vulnerabilities in WhatsUp Gold On September 24, the WhatsUp Gold team released a security advisory addressing six vulnerabilities of various severities, the most critical reaching the score of 9.8 out of 10. See CERT-EU's SA 2024-105.

All CERT-EU's Security Advisories are available to the public on CERT-EU's website, `https://www.cert.europa.eu/publications/security-advisories/`

1. Conclusions or attributions made in this document merely reflect what publicly available sources report. They do not reflect our stance.

TLP definition

TLP	Disclosure	Message
RED	Not for disclosure, restricted to participants only.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
AMBER	Limited disclosure, restricted to participants' organisations and their clients.	Recipients may share TLP:AMBER information only with members of their own organisation and its clients.
AMBER+STRICT	Limited disclosure, restricted to participants' organisations.	Recipients may share TLP:AMBER+STRICT information only with members of their own organisation.
GREEN	Limited disclosure, restricted to the community.	Subject to standard copyright rules, TLP:GREEN information may be distributed with peers and partner organisations within their sector or community, but not via publicly accessible channels.
CLEAR	Disclosure is not limited.	TLP:CLEAR information may be distributed freely.