Cyber Security Brief (June 2024)

July 1, 2024 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 402 open source reports for this Cyber Security Brief[1].
- Relating to **cyber policy and law enforcement**, the EU Council sanctioned six individuals with links to Russia for cyberattacks against member states and Ukraine, German report warned of the escalating cyber threats from APT27, APT28, and Charming Kitten, and an EU Innovation Hub report highlights challenges in criminal investigations due to encrypted communications and emerging technologies. In the US, the Biden administration banned sales of Kaspersky Lab Software, and Microsoft acknowledged responsibility for US government security breaches.
- On the **cyberespionage** front, in Europe, China-linked SneakyChef reportedly used RATs to target Ministries of Foreign Affairs, and several reportedly Russia-linked threat actors were active in cyberespionage campaigns, namely BlueDelta group that targeted European networks, APT29 that compromised TeamViewer, and several groups targeting Ukraine. Globally, Microsoft notified affected customers of e-mail conversations with Microsoft having been exfiltrated by APT29, there were several reports about alledgedly China-linked threat actors' operations.
- Relating to **cybercrime**, in Europe, the most active ransomware operations were Ransomhub, Dragonforce, Cactus, Blackbasta, Arcusmedia, while the most targeted sectors were technology, manufacturing, legal & professional services, transportation, and food.
- There were many **information operations** throughout Europe, namely Russia-aligned targeting of all 27 EU countries ahead of the European elections, as well as targeting of France due both to their legislative elections and to the Summer Olympics. Elsewhere, Russia-linked disinformation campaigns were also uncovered, and one was found targeting the US through fake CIA videos.
- As regards **data exposure and leaks** incidents, Google reportedly suffered a data leak, while Ticketmaster confirmed a breach after stolen data was found for sale online.
- On the **hacktivism** front, there were DDoS attacks in at least 16 EU countries during the European Elections.

- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in June 2024.

Europe

Cyber policy and law enforcement

Six individuals added to EU sanctions list for malicious cyber activities against EU member states and Ukraine
On June 24, the EU Council added six individuals to its sanctions list for cyberattacks against member states and Ukraine. These include members of the Russia-linked threat actors Callisto and Armageddon, as well as operators of Conti and Trickbot malware. The measures include asset freezes and travel bans. `sanctions` `russia`

German intelligence report 2024: escalating cyber threats from APT27, APT28, and Charming Kitten
On June 17, the German domestic intelligence agency (BfV) released the "2024 Report on the Protection of the Constitution" highlighting increased cyber threats. The report detailed heightened ransomware attacks, espionage by state-backed groups such as China's APT27, Russia's APT28, and Iran's Charming Kitten, hacktivism linked to the Ukraine conflict, and targeted attacks on Iranian dissidents living in Germany. The BfV called for strategic realignment and significant investments in cyber defence. `iran` `russia` `china`

EU Innovation Hub report highlights challenges in criminal investigations due to encrypted communications and emerging technologies
On June 10, the EU Innovation Hub for Internal Security published a report addressing the challenges posed by encrypted communications, quantum computing, cryptocurrencies, biometric data, AI, and large language models in criminal investigations. The report highlights the difficulties law enforcement agencies face with encrypted platforms like EncroChat and SkyECC, the increasing complexity of tracing illicit cryptocurrency transactions, and the dual impact of advanced technologies on both strengthening and weakening encryption. `encryption`

Poland's government seizes devices used to operate Pegasus spyware from Central Anti-corruption Bureau
On June 18, Poland's National Prosecutor's Office seized several devices that were used to operate Pegasus spyware from the Central Anti-corruption Bureau (CBA). The National Prosecutor's Office also acquired documents concerning Pegasus spyware purchases from the CBA, Internal Security Agency, and the Military Counterintelligence Service. The seized devices were sent for forensic analysis. High-profile Polish leaders were asked to testify on the use of Pegasus. `seizure` `psoa`

EU and US take down servers belonging to the Islamic State
On June 17, Europol, the FBI, and the US Department of Justice announced a partnered action that resulted in the largest global disruption of online critical infrastructure used by the Islamic State (ISIS) to disseminate propaganda and terrorist communications. The action brought down servers in several countries including Germany, Iceland, the Netherlands, and the US. `take down`

Cyberespionage

China-linked SneakyChef uses SugarGh0st RAT to target Ministries of Foreign Affairs
On June 21, Cisco Talos disclosed a new cyberespionage group they named SneakyChef, that has targeted Ministries of Foreign Affairs (MFA) and embassies all over the world, including in Latvia since at least August 2023. This campaign is still ongoing, with new targets despite the same malware strains SpiceRAT and SugarGh0st (Gh0stRAT variant), and tactics being used. `china` `diplomacy`

GRU's BlueDelta targets European networks in multi-phase espionage campaign
On May 30, Recorded Future reported that GRU's BlueDelta group conducted a multi-phase espionage campaign from April to December 2023. The group reportedly targeted European networks with Headlace malware and credential-harvesting web pages and used phishing, compromised internet services, and legitimate binaries to steal information, focusing on Ukraine's Ministry of Defence, European transport infrastructure, and an Azerbaijani think tank. `russia`

FlyingYeti phishing campaign targeting Ukraine
On May 30, Cloudflare reported details on a Russia-aligned threat actor FlyingYeti phishing campaign targeting Ukraine. The FlyingYeti campaign capitalised on the anxiety of Ukrainians over the potential loss of access to housing. If they open malicious files via debt-themed lures, the files would result in infection with the PowerShell malware known as Cookbox, allowing FlyingYeti to support follow-on objectives, such as installation of additional payloads and control over the victim's system. `russia`

Russia-linked APT29 compromises TeamViewer corporate IT network
On June 27 and 28, TeamViewer, a Germany-based company that has a remote access and remote control software of the same name, announced it suffered a compromise of their internal corporate IT network. TeamViewer attributed the compromise to APT29, revealing the initial access was made through the compromise of credentials of an employee account. `russia` `technology`

UAC-0200 targets defence companies in Ukraine
On June 4, CERT-UA reported about targeted cyberattacks against civil servants, military, representatives of defence enterprises of Ukraine using the malicious program DarkCrystal remote access trojan (RAT), which is distributed by means of messenger Signal. `defence`

APT attack targeting the network of the CDU German political
On June 1, the German Ministry of Interior (Bundesministerium des Innern und für Heimat) disclosed a serious cyberattack on the network of the CDU, a German political party. They said that BSI / CERT-Bund and the Federal Office for the Protection of the Constitution are working intensively to ward off the attack, investigate it and prevent further damage. `political parties`

Rafel RAT Android malware exploiting devices for cyberespionage and ransomware operations
On June 20, Check Point revealed that Rafel RAT, an Android malware, is used in espionage and ransomware campaigns. The malware targets devices in the United States, China, Indonesia, and European countries, including Romania. Rafel RAT enables remote access, data exfiltration, location tracking, and two-factor authentication bypass, impacting high-profile sectors like the military and government infrastructure.

Cybercrime

Sophisticated V3B phishing kit targets European financial institutions, enhancing threat landscape
On June 4, researchers reported the emergence of a new phishing kit named V3B, which is being

used to target 54 financial institutions across multiple European countries, including Germany, France, and Italy. The kit, offered for 130-450 US dollars per month, features advanced capabilities such as encryption, stealing of OTPs and 2FA codes, live victim interaction, and uses PhotoTAN and SmartID bypass methods, signalling a sophisticated Phishing-as-a-Service (PaaS) operation. `phishing kit`

Ransomware attack disrupts London hospitals
On June 3, according to the BBC, a ransomware attack on Synnovis, a provider of pathology services, severely disrupted multiple NHS hospitals in London. The attack impacted blood transfusions and other critical services, leading to the cancellation and redirection of some medical procedures. Emergency care remained available. Media reports have linked Qilin ransomware to the attacks. `health`

StrelaStealer resurgence targets European email credentials
On June 24, SonicWall Capture Labs reported on the significant rise of StrelaStealer, which targets European users by stealing Outlook and Thunderbird e-mail credentials. This malware avoids Russian systems by checking the system's keyboard layout. It operates by initially infecting with an obfuscated JavaScript file via e-mail, which then releases a DLL that injects the stealer into the process. The malware particularly targets users in Poland, Spain, Italy, and Germany. `russia`

Information operations

Russian and Iranian influence networks target French legislative elections
On June 28, Recorded Future reported that Russian and Iranian influence networks are targeting the French legislative elections, with minimal impact so far. The Russia-linked Doppelgänger network employs cloned websites and social media bots to impersonate French media, spreading pro-Russian and eurosceptic content. The CopyCop network, using AI, manipulates articles from legitimate sources to undermine President Macron. Iran's involvement, through a network called International Union of Virtual Media, is limited, likely due to France's support for Israel. `iran` `russia` `election`

Russia-aligned information operations aim to undermine the summer Olympics
On June 2, Microsoft reported that a Russia-aligned information operation is focusing on spreading negative narratives relating to the summer Olympics in France. One of the messages spread was a fake Tom Cruise persona which was disparaging the International Olympic Committee's leadership. `russia`

Pro-Russia Pravda disinformation campaign targets all 27 EU countries
On June 3, 2024, the European Digital Media Observatory (EDMO) reported on a Russian disinformation campaign targeting the EU elections. This campaign, linked to the Russian state-controlled media outlet Pravda, involved a network of fake news sites and social media accounts spreading false information across Europe. The campaign utilised AI-generated content and deepfake videos to influence public opinion, targeting all 27 EU countries and some non-EU countries. `russia` `election`

Euromore: Russia's new information warfare tool
On June 2, Le Monde reported about Kremlin-linked organisations creating Euromore to replace banned Russian state media RT and Sputnik in Europe. Launched in March 2022, Euromore presents itself as an independent European outlet but is actually funded by Pravfond and Rusfuture, both close to Russian intelligence. Euromore disseminates pro-Russian narratives and combats anti-Russian sentiments, illustrating a significant shift in Russia's information operations in response to European sanctions. `russia`

Polish State News Agency breached; Poland authorities claim attack likely Russia-backed
On May 31, Polish authorities reported that the state-owned Polish Press Agency (PAP) experienced a cyberattack. A threat actor posted a false article to the PAP's website stating Polish Prime Minister Donald Tusk ordered a "partial mobilisation" to begin on July 1, 2024. Polish authorities claimed the breach was part of a Russia-backed information operation ahead of the upcoming June 2024 EU elections. `russia` `election`

Moldovan brothers own UK-based shell company reportedly involved in Russian influence operations in Europe
0n May 31, researchers at Correctiv revealed that the Neculiti brothers from Moldova support Russia's cyber warfare against Europe through their web-hosting company PQ Hosting. These services are used for disinformation campaigns and cyber attacks. Despite international sanctions, their operations circumvent restrictions. They claim that Stark Industries Solutions, a company previously reported to have been involved in similar activities, is a shell company for PQ Hosting. `russia`

Hacktivism

DDoS attacks in at least 16 EU countries and a Union entity during European Parliament Elections
During the European Parliament Elections which took place from June 6 to June 9, a collective of pro-Russia supposed hacktivists, including NoName057(16), HackNeT, and Russian Cyber Army conducted DDoS attacks on the websites of organisations in 16 EU countries and two Union entities. The attacks were mostly focused on public transport infrastructure in many EU countries, a few public administrations and a legislative body. `russia` `transport` `election` `public administration`

Russia-linked hacktivists target Romania
On June 17, Cyber Army of Russia announced on Telegram they were starting a DDoS campaign targeting several services in Romania, starting with the port of Constanza. They did this in response to the country's denial of visas to a Russian delegation to attend the OSCE Parliamentary Assembly. `russia`

World

Cyber policy and law enforcement

AWS introduces FIDO2 passkeys and mandates MFA for root accounts by July 2024
On June 12, Amazon Web Services (AWS) announced that it has introduced FIDO2 passkeys for multi-factor authentication (MFA) to enhance account security and usability, offering resistance to phishing and man-in-the-middle attacks. AWS has also reminded users that root accounts must enable MFA by the end of July 2024, with a phased rollout beginning initially for root users and expanding over time. `multi-factor authentication`

AI jailbreaks
On June 4, Microsoft shared details about AI jailbreaks. AI jailbreaks are attacks that can circumvent safeguards, causing AI systems to produce harmful or unintended outputs. Such vulnerabilities arise from overconfidence, gullibility, and susceptibility to manipulation. Mitigation involves layered defences like prompt filtering, identity management, and abuse monitoring. Microsoft's approach includes a zero-trust model and the use of tools like PyRIT for risk identification. `artificial intelligence`

Hong Kong arrests activists who commemorate Tiananmen Square protests on social media
In late May, Hong Kong law enforcement detained six individuals under a recent security law for social media posts inciting hatred against Beijing. The posts related to the Tiananmen Square protest anniversary on 4 June. This law, expanding government powers over broadly defined offences, aligns Hong Kong with China's security framework. `social media` `china`

Iran approves the creation of National Artificial Intelligence Organisation
On June 20, Iran announced its approval for creating the National Artificial Intelligence Organisation (NAIO) as well as an AI steering council. The decision has been made by the Vice President for Science, Technology, and Knowledge-Based Economy where he also stated a 10-year roadmap to boost Iranian AI technologies as Khamenei has declared that Iran aims to be among the top 10 nations to secure its influence in artificial intelligence. `iran` `artificial intelligence`

YouTube removes Iranian Foreign Ministry's account Over US sanctions compliance
On May 28, a YouTube spokeswoman confirmed that the video platform terminated an account run by Iran's Foreign Ministry to comply with US sanctions against the Islamic republic. The spokeswoman elaborated that Google is committed to compliance with applicable sanctions and trade compliance laws, and enforces related policies under their terms of service. `sanctions` `iran`

Biden bans US sales of Kaspersky software over Russia ties
On June 20, the Biden administration announced a ban on US sales of Kaspersky Lab software, effective September 29, due to security concerns over Russian influence. Kaspersky denies the allegations and plans legal action. The ban covers downloads, resales, and licensing to mitigate cyberattack risks amid Ukraine war tensions. On June 21, OFAC sanctioned 12 Kaspersky Lab executives for operating in Russia's technology sector. `ban` `russia` `united states`

Microsoft acknowledges responsibility for major 2023 US government hack
On June 13, The Washington Post reported that Microsoft President Brad Smith acknowledged the company's responsibility for a major hack of US government systems that occurred last year. In his testimony before Congress, Smith promised to enhance security practices and accepted findings from an investigation linking the breach to Chinese hackers. Despite criticism, Microsoft's products remain indispensable for both corporate and federal operations due to their deep integration. `united states` `russia` `china` `public administration`

Microsoft reportedly ignored security flaw to secure federal contract
According to a June 13 report by ProPublica, an independent investigative newsroom, Microsoft hired cybersecurity expert Andrew Harris for his skills in protecting sensitive networks. In 2016, Harris discovered a critical flaw in a Microsoft application that allowed undetected data breaches. Despite his warnings, Microsoft prioritised securing a multibillion-dollar US government contract over fixing the issue, resulting in vulnerabilities exploited in the 2020 SolarWinds hack. Frustrated by inaction, Harris left Microsoft in 2020. `united states`

The US Department of Justice is offering a 10 million US dollars reward for information about GRU hacker
On June 26, the US has indicted Russian national Amin Timovich Stigal for cyberattacks on Ukrainian government networks, linked to the GRU before Russia's invasion. Stigal distributed WhisperGate malware and exfiltrated sensitive data. His activities are also linked to operations targeting NATO and the US. A million US dollars reward is offered for information leading to his arrest. If convicted, he faces up to five years in prison. `reward` `russia` `united states`

US dismantles 911 S5 botnet
On May 29, US FBI reported that they dismantled the 911 S5 botnet and arrested its administrator in a coordinated international law enforcement action. In the unsealed indictment

they allege that the administrator and others created and disseminated malware to compromise and amass a network of millions of residential Windows computers worldwide. These devices were associated with more than 19 million unique IP addresses, including 613.841 IP addresses located in the United States. `dismantle`

Cyberespionage

Microsoft notifies customers about e-mail exfiltration by APT29
On June 28, Reuters reported that Microsoft notified customers about the consequence of a cyberattack by the Russia-linked APT29 (aka Midnight Blizzard) threat actor, which occurred between late November 2023 and January 2024. The threat actor used a password spray attack to infiltrate Microsoft's e-mail systems, accessing e-mails exchanged between the company and its customers. Microsoft detected the breach on January 12, 2024, and is now notifying affected clients while taking measures to enhance its security systems. `russia`

Sophos finds overlap in infrastructure and tools between at least three China-linked intrusion sets
On June 5, Sophos reported uncovering a complex, long-running Chinese state-sponsored cyberespionage operation in May 2023. The operation targeted a high-profile government organisation in Southeast Asia, tracking at least three intrusion clusters from March to December 2023. These clusters used tools and infrastructure linked to known Chinese threat actors, including BackdoorDiplomacy, REF5961, Worok, TA428, Unfading Sea Haze, and APT41 subgroup Earth Longzhi. `china`

UNC3886 a China-nexus cyberespionage actor exploited 4 zero days in the past few years
On June 18, Mandiant and Google Cloud detailed activity associated with UNC3886. UNC3886 is a suspected China-nexus cyberespionage actor who exploited FortiOS and VMware vulnerabilities towards strategic targets globally between 2021 and 2024. UNC3886's activities include exploiting CVE-2023-34048 (VMware vCenter) since late 2021 as well as three other zero-days. `china`

China-linked threat actor Velvet Ant abuses F5 Load Balancers for persistence
On June 17, Israel-based security company SYGNIA published a report on China-linked threat actor Velvet Ant compromising the network of a large organisation in late 2023. They infiltrated the network for about three years, maintaining multiple footholds, including using a legacy F5 BIG-IP appliance. `china`

AridViper APT targeting Android users with spyware
On June 13, ESET reported five campaigns targeting Android users with trojanised apps since at least 2022, attributed to the AridViper group known to be targeting entities in the Middle-East. They deploy multistage Android spyware, dubbed AridSpy, that downloads first- and second-stage payloads from C2 servers. The malware is distributed through dedicated websites impersonating various messaging apps, a job opportunity app, and a Palestinian Civil Registry app. `middle east`

Pakistan-linked threat actor UTA0137 uses Discord-based malware to target Indian government
On June 13, Volexity reported on Pakistan-linked threat actor UTA0137 using DISGOMOJI malware to target the Indian government. DISGOMOJI is a fork of discord-c2 malware that uses Discord for C2, employs emojis for communication. UTA0137 also utilised DirtyPipe exploit for privilege escalation on the Linux BOSS distribution. Volexity assesses UTA0137's campaign as successful. `pakistan` `india`

Cybercrime

OTP bots bypass 2FA via phishing and social engineering

On June 10, Kaspersky reported that phishing schemes using one-time password (OTP) bots are increasingly bypassing two-factor authentication by tricking victims into revealing OTP through social engineering tactics. Attackers use OTP bots to impersonate trusted organisations, make convincing calls to victims, and retrieve OTPs to gain unauthorised access to accounts, underscoring the need for enhanced vigilance and protective measures against such scams. `phishing`

LockBit falsely claimed to have breached the US Federal Reserve

On June 23, the LockBit ransomware group falsely claimed to have breached the US Federal Reserve, stealing 33 terabytes of sensitive data. It was later revealed they had actually targeted Evolve Bank & Trust. The bank confirmed the breach and is addressing the issue, offering credit monitoring to affected customers. `ransomware`

P2Pinfect botnet targets Redis and deploy new ransomware

On June 25, Cado Security reported on P2Pinfect, a sophisticated Rust-based malware, using a peer-to-peer botnet for its command-and-control mechanism. Initially appearing dormant and spreading via Redis and limited SSH, the malware has recently been updated to include ransomware and a crypto miner payload. P2Pinfect exploits Redis replication to gain code execution, scans for more servers, and uses SSH for further spread. `ransomware`

Malicious npm package targets AWS users with backdoor

On June 26, ReversingLabs researchers published a report on a malicious npm package, legacyreact-aws-s3-typescript, targeting AWS users by mimicking a popular legitimate package. This package, dormant for four months, contained a postinstall script downloading a backdoor. `supply-chain attack`

NetSupport delivered through MSIX packages

On June 17, SANS ICS reported a NetSupport campaign using MSIX packages to deliver a malicious client, bypassing the need for custom C2 infrastructure. The campaign uses a portable 7zip version to install the client and targets Microsoft domains. Attributed to the cybercrime Sangria Tempest group, this attack abuses advertisement networks and MSIX installers. `supply-chain attack`

Data exposure and leaks

Google reportedly suffers data leak

On June 3, 404 Media, an independent digital media company, reported that Google experienced a leak of an internal database containing thousands of security and privacy incident reports from employees. These incidents included accidental recordings of children's voices and other sensitive data breaches. `technology`

Cybercrime actor intrude and extort Snowflake customers

On June 10, Mandiant reported that UNC5537 has targeted Snowflake customer database instances for data theft and extortion. Snowflake is a multi-cloud data warehousing platform. UNC5537 is a financially motivated actor who compromised Snowflake customer instances using stolen credentials. They are selling victim data on cybercrime forums and attempting extortion, having allegedly stolen a significant volume of records from Snowflake customer environments. `technology`

Ticketmaster confirms massive breach after stolen data for sale online

On May 20, Live Nation confirmed that Ticketmaster, a ticket sales and distribution platform,

suffered a data breach after its data was stolen from a third-party cloud database provider, which is believed to be Snowflake. The breach has allegedly exposed the data of over 560 million Ticketmaster users. A threat actor known as Shiny Hunters is attempting to sell the Ticketmaster data on a hacking forum for 500.000 US dollars. `entertainment`

AI platform Hugging Face breached
On May 31, AI platform Hugging Face revealed that its Spaces platform was breached, allowing hackers to access authentication secrets for its members. Hugging Face Spaces is a repository of AI apps created and submitted by the community's users, allowing other members to demo them. Hugging Face revoked authentication tokens in the compromised secrets and notified those impacted by email. However, they recommend that all users refresh their tokens. `artificial intelligence`

Information operations

Chinese info ops targets daughter of exiled critic
On June 27, the New York Times reported that a prominent Chinese writer who lives in exile in the US and who regularly criticises China and its leader has become the target of a cover influence operation on social media. The critic's teenage daughter has become subject to vulgar commentary on her social media accounts across X, Facebook, TripAdvisor, Patch, and even Niche, a website that helps parents choose schools. The report suggests that the vulgar comments are part of a coordinated Chinese influence operation associated to China's security services. `china`

Pakistani APTs escalate attacks on Indian government
On April 24, Seqrite Labs reported an escalation in cyberattacks on Indian government entities by Pakistan-linked APTs, particularly SideCopy and Transparent Tribe (APT36). These groups reportedly used various RATs, including AllaKore and Crimson, in multiple campaigns. Techniques involved spearphishing and leveraging compromised domains for payload delivery. Seqrite reported that the attacks are part of broader disinformation and influence operations aimed at destabilising Indian governmental and defence sectors. `india` `world`

Pravfond: a facade for Russian cyber operations and disinformation campaigns
On June 2, 2024, an investigation by a consortium of newspapers, including DR and Le Monde, uncovered that Pravfond, a Russian organisation that purports to assist expatriates, is predominantly involved in financing legal defences for Kremlin-aligned individuals and suspected spies. The investigation revealed Pravfond's deep ties with Russian intelligence agencies and its participation in disinformation campaigns against Ukraine and anti-Western propaganda, underscoring its significant role in Russia's global geopolitical and intelligence strategies. `russia`

Fake CIA video from Russia sources aiming at spreading misinformation
On June 19, CBS and other news outlets reported that a fake CIA video was circulating, warning Americans about a "high risk" of attacks on the Paris metro. This comes in light of efforts of disinformation campaigns from Russia against the Paris Olympics. The video originated from Russian sources before spreading to social media where it accumulated at least 100.000 views. `russia`

Israel reportedly targets US lawmakers with covert influence operation
On June 5, the New York Times revealed Israel's 2 million US dollars covert influence campaign targeting US lawmakers and the public to support Gaza war actions. Managed by the Ministry of Diaspora Affairs and Stoic, the operation used fake accounts on social media to post pro-Israel comments, particularly targeting Black Democratic lawmakers. The campaign, identified by FakeReporter, was disrupted by Meta. `israel` `united states`

Significant vulnerabilities

Confluence Data Center and Server Remote Code Execution
A critical remote code execution (RCE) vulnerability, CVE-2024-21683, has been discovered in Atlassian's Confluence Data Center and Server. This vulnerability allows authenticated attackers with privileges of adding new macro languages to execute arbitrary code. See CERT-EU's SA 2024-054.

SolarWinds High-Severity Vulnerabilities
On the 4th and 5th of June 2024, SolarWinds published four separate security advisories related to high-severity vulnerabilities in multiple products. CERT-EU strongly recommends patching them as soon as possible. See CERT-EU's SA 2024-055.

Multiple Vulnerabilities in Microsoft Products
On June 11, 2024, Microsoft addressed 58 vulnerabilities in its June 2024 Patch Tuesday update, including one zero-day vulnerability. This Patch Tuesday also fixes one critical vulnerability, a Microsoft Message Queuing (MSMQ) Remote Code Execution vulnerability. See CERT-EU's SA 2024-056.

Vulnerabilities in JetBrains Products
On June 10, JetBrains released a fix for a vulnerability affecting IntelliJ-based IDEs 2023.1+ and JetBrains GitHub Plugin. This vulnerability could lead to disclosure of access tokens to third-party sites. See CERT-EU's SA 2024-057.

Vulnerabilities in PHP
On June 6, 2024, a critical vulnerability was identified in certain versions of PHP that could allow the execution of arbitrary code or disclosure of sensitive information on Windows systems using Apache and PHP-CGI. The vulnerability is currently being actively exploited, and several proof of concepts are available. See CERT-EU's SA 2024-058.

Vulnerability in FortiOS
On June 12, 2024, Fortinet disclosed a high-severity vulnerability identified as CVE-2024-23110 affecting FortiOS. This vulnerability allows an authenticated attacker to execute unauthorised code or commands via specially crafted command line arguments. The issue arises from multiple stack-based buffer overflow security defects in the command line interpreter. See CERT-EU's SA 2024-059.

Vulnerabilities in VMware Products
On June 17, 2024, VMware released fixes for three vulnerabilities affecting VMware vCenter Server and VMware Cloud Foundation. Two of these vulnerabilities are critical. Exploitation these vulnerabilities could allow a malicious actor to execute remote code or escalate privileges on the affected systems. See CERT-EU's SA 2024-060.

Vulnerabilities in Nextcloud Products
On June 14, 2024, Nextcloud released patches for Nextcloud Server and Enterprise Server. A vulnerability was disclosed in Nextcloud server products that allows the bypassing of the second factor of two-factor authentication (2FA). See CERT-EU's SA 2024-061.

Vulnerabilities in Chrome and Chromium based Browsers
Google has released a critical security update for its Chrome Browser, addressing six high-severity vulnerabilities that could lead to serious security issues. Chromium-based browsers are also impacted. See CERT-EU's SA 2024-062.

Critical Vulnerability in MOVEit Transfer
On June 25, 2024, Progress Software disclosed a critical vulnerability in Progress MOVEit Transfer. This vulnerability allows attackers to bypass authentication and access sensitive data.

The vulnerability is actively being exploited, and there is an available proof of concept (PoC). See CERT-EU's SA 2024-063.

Vulnerabilities in GitLab
On June 26, 2024, GitLab released a security advisory addressing several vulnerabilities, one of which being critical, allowing an attacker to trigger a pipeline as another user under certain circumstances. See CERT-EU's SA 2024-064.

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 it's 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.