Cyber Brief (May 2024)

June 3, 2024 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 336 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, in Europe, Belgium will oversee compliance of Telegram with the EU's Digital Services Act, Germany, the Czech Republic and the Council of the European Union condemned APT28 cyberattacks and Europol, France, Germany and the Netherlands conducted a coordinated law enforcement operation against a malware dropper ecosystem. Elsewhere, UK, US and Australian law enforcement identified and sanctioned the Lockbit leader, TikTok expanded global restrictions on covert influence operations, Iran reintroduced internet-restrictive legislation, and the FBI seized BreachForums.
- On the **cyberespionage** front, in Europe, a Belgian MP was infected with spyware, Russia-linked APT28 targeted the Polish government and Pegasus spyware was used against Russian and Belarusian-speaking opposition activists. Elsewhere, Pakistan-linked malware targeted entities in India, China-linked campaigns targeted governmental entities in the South China Sea region, Iran-linked APT42 targeted Western academia, Amnesty International exposed Indonesian spyware activities, an Israel-linked campaign against the ICC was revealed, multiple Rwandan officials were targeted with Pegasus spyware, and the SugarGh0st RAT was used against US AI organisations.
- Relating to **cybercrime**, in Europe, the most active ransomware operations were Lockbit 3, Akira, Cactus, Blackbasta and Ransomhub, while the most targeted sectors were technology, manufacturing, construction & engineering, healthcare and education.
- As regards **data exposure and leaks**, Banco Santander reportedly suffered a breach affecting customers and employees in Spain, Chile, and Uruguay, while the UK Ministry of Defence reportedly experienced a breach exposing Armed Forces personnel data. Companies such as Dropbox, Microsoft, Dell, Ticketmaster, and Hugging Face reportedly experienced unauthorised access to their systems.
- On the **hacktivism** front, pro-Russia supposed hacktivists intensified DDoS attacks on Sweden amid its NATO membership pursuit, and targeted Kosovo government websites in retaliation for supporting Ukraine. Stark Industries Solutions was reported to support NoName057 by facilitating DDoS attacks.

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

Europe

Cyber policy and law enforcement

Belgium authorities will oversee the compliance of Telegram to the DSA
On May 7, De Standaard, a Belgian newspaper, reported that the social media platform Telegram will be overseen by Belgian authorities to comply with the EU's Digital Services Act (DSA). It selected the European Digital Services Representative in Brussels as its legal representative. The Belgian telecoms authority BIPT will monitor Telegram, which has over 800 million users but has faced criticism for enabling harmful content. `regulation`

France blocks Tiktok domains in New Caledonia
On May 15, the French government temporarily banned the social media platform TikTok in New Caledonia following the recent riots as part of a state of emergency which includes the deployment of the army and a curfew on the island of around 270.000 inhabitants. This ban involves New Caledonia's state-run Postal and Telecommunication Service blocking TikTok domains. `france` `ban`

Germany, Czechia and the EU condemn cyberattacks by Russia-linked APT28
On May 3, the German foreign minister attributed a cyberattack targeting various e-mail accounts of the German Social Democratic Party executive in 2023 to Russia-linked APT28. Czechia also attributed a cyberattack on Czech institutions exploiting a previously unknown vulnerability in Microsoft Outlook from 2023 to APT28. The Council of the European Union released a statement strongly condemning the cyberattacks. `russia` `election` `public administration`

Europol coordinates law enforcement operation rolling up dropper malware ecosystem
Between May 27 and 29, Europol coordinated operation Endgame together with law enforcement partners from the Netherlands, France and Germany. They targeted droppers like IcedID and Trickbot and focused on dismantling computer networks used to spread ransomware via infected emails. High-value arrests, server seizures, and the freezing of illegal assets marked significant impacts on the dropper ecosystem, linked to ransomware and other malware attacks. `law enforcement`

Cyberespionage

Belgian MP who focuses on China matters was infected with spyware for months
On May 23, Belgian MP Goedele Liekens reported being spied on for months, suspecting Chinese actors. As part of a Parliamentary Committee on China, she recently visited Taiwan and investigated Uighur mistreatment. Her laptop, phone, and tablet were infected with spyware, discovered two weeks before the Belgian parliamentary election. The infection came through a spearphishing e-mail from a fellow Belgian MP. `china` `election`

APT28 targets Polish government
In early May, CERT-PL observed Russia-linked APT28 conduct a malware campaign against Polish government institutions using deceptive e-mails to deliver malicious links. The attacks leverage free and common developer services to obscure the campaign's activities and deploy sophisticated malware to execute further illicit actions on compromised systems. `russia` `public administration`

APT28 continues to target European entities

On May 30, Recorded Future reported on Russia-linked APT28 conducting credential-stealing campaigns targeting Ukraine's Ministry of Defence, Ukrainian weapons import and export companies, European railway infrastructure enterprises, and a think tank based in Azerbaijan. The threat actor continues to deploy Headlace malware, abusing legitimate services such as GitHub, Mocky, and InfinityFree. Credential harvesting campaigns targeted webmail service users, using scripts hosted on compromised routers to defeat two-factor authentication and CAPTCHA challenges. `russia` `public administration`

Pegasus targeting of Russian and Belarusian-speaking opposition activists and independent media in Europe

On May 30, a joint investigation revealed that seven Russian and Belarusian-speaking journalists and activists in Europe were targeted with NSO Group's Pegasus spyware from August 2020 to January 2023, potentially by a single NSO customer. `russia` `psoa`

Cybercrime

Threat actor targeting financial organisations in Europe through Microsoft Minesweeper

On May 26, CERT-UA and CSIRT-NBU (Ukraine's national bank) reported that a threat actor named UAC-0188 is exploiting a Python clone of Microsoft's Minesweeper game to conceal malicious scripts targeting financial organisations in Europe and the US. At least five breaches have been reported. They are using the legitimate game code to hide Python scripts that download and install SuperOps RMM, a legitimate remote management software. `finance`

Information operations

France warns Ireland of Russian disinformation targeting Irish voters

On May 11, French officials informed the Irish Department of Foreign Affairs about Russia's expansion of disinformation campaigns into Ireland, targeting the upcoming European elections. This network of Russian websites and social media accounts aims to stir discord in EU countries by capitalising on contentious topics like immigration. The activity, which began impacting Ireland since March, has intensified as the elections approach. `election`

Polish State News Agency breach is 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. `election` `russia`

Data exposure and leaks

Banco Santander reported a data breach

On May 15, Banco Santander S.A. reported a data breach affecting customers and employees in Spain, Chile, and Uruguay. The breach occurred when an unauthorised party accessed a database managed by a third-party service provider. While the bank confirmed that the breach did not compromise transaction details or online banking credentials, it did not specify which types of data were exposed. `finance`

UK Ministry of Defence breach exposes personnel data

On May 7, the UK Ministry of Defence confirmed a recent data breach. A threat actor gained

access to part of the Armed Forces' payment network. While the breach affected personal data of active and reserve personnel and some retired veterans, the Defence Secretary assured minimal impact on salaries, expenses, and pensions, with an investigation underway to determine the breach's origin, including potential foreign state involvement, notably from China. `china`

Hacktivism

Surge of DDoS attacks targets Sweden amid NATO pursuit
On May 2, Netscout, an IT company, reported that Sweden faced more DDoS attacks since it pursued NATO membership. The peak reportedly occurred on March 4, with Netscout recording 2275 attacks in a single day. Pro-Russia supposed hacktivist groups have claimed the attacks.

Pro-Russia supposed hacktivists are targeting OT infrastructure of water facilities in Europe
On May 1, the US, UK and Canadian governments issued a joint statement in which they report that pro-Russia hacktivists are conducting attacks against operational technology (OT) devices in North America and Europe. The hacktivists reportedly seek to compromise modular, internet-exposed industrial control systems (ICS) through their software components, such as human-machine interfaces (HMIs), by exploiting virtual network computing (VNC) remote access software and default passwords. `russia`

Pro-Russia supposed hacktivists DDoS government websites of Kosovo
Between May 7 and 8, pro-Russia supposed hacktivists conducted DDoS attacks against governmental entities in Kosovo including the website of the Presidency and the Prime Minister. Some governmental websites experienced temporary downtime during the attacks. The Defence Minister of Kosovo stated that the attacks were retaliation for his statement of support to Ukraine at the Defence 24 conference in Poland. Kosovo pledged to provide military equipment to Ukraine. `russia` `ukraine war`

World

Cyber policy and law enforcement

Iranian parliament reintroduces legislation that would further restrict internet access
On May 12, Iran's parliament reintroduced the Legislation to Protect Cyberspace Users, first halted in 2022, which would increasingly restrict Iran's internet access. The bill could impede access to international services, jeopardise net neutrality, and potentially impede Iranians from utilising VPNs. `legislation` `iran`

US, UK and Australian law enforcement identify and sanction Lockbit leader
On May 7, US, UK and Australian law enforcement reported that the leader of Lockbit ransomware operations has been identified and sanctioned. The announcement was made following an international disruption campaign from law enforcement agencies. `sanction`

TikTok expands restrictions on state-affiliated influence operations globally
On May 23, TikTok announced it would further limit the reach of state-affiliated covert influence operations. The platform, which started labeling such media in 2022, has disrupted 15 influence operations and removed over 3.000 accounts this year alone. The move is part of efforts to safeguard political discourse during a significant election year, with four billion people voting across 76 countries. `restriction` `election` `social media`

BreachForums seized by the FBI
On May 15, the FBI confiscated BreachForums, a notorious hacking forum known for distributing

and selling stolen corporate data. As of May 16, the forum was displaying a notice indicating FBI control over its website and backend data. Additionally, the FBI has taken control of the forum's Telegram channel, posting messages confirming their oversight. `seizure` `united states`

US Department of Justice charges five individuals for their roles in cyber schemes that funded North Korea's nuclear weapons program
On May 16, the US Department of Justice charged five individuals, a US citizen, a Ukrainian citizen, and three other foreign nationals, for their roles in cyber schemes that funded North Korea's nuclear weapons program. Between October 2020 and October 2023, these individuals allegedly participated in a campaign coordinated by the North Korean government to fraudulently infiltrate US job markets to generate revenue for the regime's illicit nuclear activities. `charges` `united states` `north korea`

Cyberespionage

China-linked Unfading Sea Haze targets military and governmental entities in the South China Sea region
On May 22, Bitdefender reported on Unfading Sea Haze, a previously unknown threat actor aligning with Chinese geopolitical interests, that has targeted military and government entities in the South China Sea since 2018. The threat actor's attacks started with spearphishing e-mails, leveraging MSBuild for fileless malware, and maintaining persistence through hidden admin accounts. They used various tools, including Gh0stRAT variants and custom exfiltration methods. `china`

Chinese cyberespionage campaign targeting governmental entities in Africa, Asia and the Middle East
On May 23, Palo Alto Networks reported an active Chinese cyberespionage campaign targeting governmental entities in Africa, Asia and the Middle East. The campaign, named Operation Diplomatic Specter, has been ongoing since late 2022. The cyberespionage efforts focus on diplomatic missions, military operations, political meetings, and high-ranking officials. `china`

China-linked threat actor Sharp Dragon expands operations to Africa and the Caribbean
On May 23, Checkpoint reported on Sharp Dragon, a China-linked threat actor that has expanded its operations to Africa and the Caribbean, targeting governmental organisations. Utilising compromised infrastructure and phishing attacks, they deploy Cobalt Strike Beacon for initial access. This strategic shift indicates a broader effort by Chinese cyber actors to enhance influence in these regions. The group's tactics show increased target selection caution, operational security, and high-profile targeting. `china`

Iran-linked APT42 threat actor targets Western academia
On May 2, Mandiant reported that APT42, an Iranian state-sponsored cyberespionage actor associated with the Islamic Revolutionary Guard Corps (IRGC) used enhanced social engineering schemes to gain access to victim networks, including cloud environments. The activity targeted Western non-governmental organisations (NGOs), media organisations and academia. `iran`

Possible Russia-linked TinyTurla malware spotted in the Philippines
On May 20, Cyble, a US-based cybersecurity company, published a report on a campaign targeting an NGO in the Philippines using malicious .LNK files disguised as human rights seminar invitations. These files, distributed via spam e-mails, embed PDFs and MSBuild project files. Russian-language code hints and targeting NGOs suggest attribution to the Russia-linked threat actor Turla. `russia`

New North Korean threat actor Moonstone Sleet targets companies for espionage and cybercrime
On May 28, Microsoft reported that North Korean threat actor Moonstone Sleet, used diverse

methods for cyberespionage and cybercrime attacks. The actor set up fake companies and job openings, used trojanised tools, developed a malicious game called DeTankWar, and deployed custom ransomware named FakePenny. Initially overlapping with Diamond Sleet, Moonstone Sleet has now developed its own distinct tactics and infrastructure. `north korea` `technology` `defence`

North Korea exploits DMARC for spoofing in social engineering towards South Asian entities
On May 2, the US FBI reported that North Korean cyberespionage actor Kimsuky targeted a South Asian entity with social engineering attacks. The attacks exploited weakly configured DNS domain-based message authentication, reporting and conformance (DMARC). The DMARC weaknesses were exploited to spoof spearphishing e-mails in their attacks. `north korea`

Pakistan-linked threat actor targets Indian critical sectors with multi-platform malware
On May 22, Blackberry researchers reported that the Pakistan-linked threat actor Transparent Tribe group initiated a series of attacks against India's government, defence, and aerospace sectors, from late 2023 to April 2024, employing malware developed in Python, Golang, and Rust. These attacks leveraged spearphishing and popular services like Discord and Google Drive. Three key Bengaluru-based companies associated with the Department of Defence Production have been identified as primary targets. `india` `pakistan` `aerospace` `public administration` `defence`

Threat actors exploit Microsoft Graph API for covert malware communications
On May 2, Symantec researchers reported that threat actors are increasingly leveraging Microsoft Graph API for malicious activities, allowing them to communicate with command-and-control infrastructure on Microsoft's cloud services while evading detection. According to the report, since January 2022, various nation-state threat actors have been observed abusing the API, including the Russia-linked APT28, the China-linked APT15 and the North Korea-linked APT37. `russia` `china` `north korea`

Israel's decade-long hacking campaign against the ICC
On May 28, The Guardian revealed that Israeli intelligence agencies conducted a decade-long campaign against the ICC, hacking and intercepting communications of ICC officials, including prosecutors Karim Khan and Fatou Bensouda. They accessed phone calls, e-mails, and documents, particularly through Palestinian telecom infrastructure. The Shin Bet reportedly installed Pegasus spyware on the phones of Palestinian NGO employees and officials. The ICC implemented countermeasures to protect their evidence and maintain security amid these hacking attempts. `israel` `legal` `psoa`

Amnesty International exposes Indonesia's spyware hub and calls for global action
On May 1, Amnesty International reported that Indonesia has become a hub for spyware and surveillance tools, threatening citizens' rights and privacy. The investigation uncovered extensive sales and deployment of invasive technologies, with Indonesian government agencies identified as buyers. `psoa`

Multiple Rwandan officials and their families targeted with Pegasus spyware
From 2019 to 2021, according to Forbidden Stories, an international network of journalists, a Rwandan opposition leader and at least 12 Rwandan political figures and their family members were targeted with NSO Group's Pegasus spyware. High-profile Pegasus targets include the advisor to the president of Rwanda as well as former Ministers of Justice and Infrastructure. Rwanda-based Pegasus operators reportedly also targeted the daughter of a prominent Belgian-based human rights activist. `psoa`

SugarGh0st RAT campaign targets organisations involved in artificial intelligence
On May 16, Proofpoint reported on a SugarGh0st RAT campaign from May aimed at US organisations involved in artificial intelligence, spanning academia, private industry, and

government sectors, targeting fewer than ten individuals. SugarGh0st RAT is a customised version of Gh0stRAT, commonly used by Chinese-speaking threat actors. Since its initial report in November 2023, only a few campaigns have been noted, and they are highly targeted. `united states` `artificial intelligence`

Justice AV Solutions supply-chain attack CVE-2024-4978

On May 23, Rapid7 reported on a backdoored version of the Justice AV Solutions (JAVS) Viewer software used in supply-chain attack. JAVS Viewer is video recording software known to be used in courtrooms, legal offices, correctional facilities, and government agencies worldwide. The JAVS Viewer v8.3.7 contained a backdoored installer, tracked as CVE-2024-4978, that allowed threat actors to gain full control of compromised systems. `supply-chain attack`

Cybercrime

Morocco-based cybercrime threat actor Storm-0539 targets gift card users

On May 23, Microsoft published a report on Morocco-based cybercrime threat actor Storm-0539 targeting gift card users. The FBI warned about their advanced techniques on May 6. Microsoft notes a 60% rise in activity last Christmas and 30% between March and May 2024. The group targets organisations issuing gift cards, using stolen accounts and cloud services for low-cost operations.

Gipy malware campaign targets global users with deceptive AI voice changer app

On May 24, Gipy malware users have been observed targeting Germany, Russia, Spain, and Taiwan through phishing schemes offering an AI voice changer app. First appearing in early 2023, this malware can steal data, mine cryptocurrency, and install additional malicious software. While the application functions as advertised, it simultaneously delivers Gipy malware, which includes numerous threats such as the Lumma password stealer, Apocalypse ClipBanker, and several remote access trojans. `artificial intelligence` `techniques`

Anatsa banking trojan resurfaces on Google Play, infecting millions

On May 27, Zscaler security researchers identified over 90 harmful Android apps with over 5.5 million downloads on Google Play that have spread malware, including the Anatsa banking trojan. Anatsa, targeting over 650 financial apps worldwide, steals e-banking credentials for fraud. `mobile malware`

Three million Docker Hub repositories contain malicious content

On April 30, JFrog, an IT company, reported that their research uncovered coordinated attacks on Docker Hub that planted millions of malicious repositories. Their research revealed that nearly 20% of these public repositories, almost three million repositories, hosted malicious content. The content ranged from simple spam that promoted pirated content, to malicious entities such as malware and phishing sites, uploaded by automatically generated accounts. `technology`

First robocall named threat actor by US

On May 13, the US Federal Communications Commission designated Royal Tiger as the first officially recognised robocall threat actor. This group, active in India, the UK, the UAE, and the US, has been involved in robocalls impersonating official agencies and offering fraudulent credit services. This designation aids international partners and law enforcement in tracking and addressing such activities. `united states`

Data exposure and leaks

Dropbox suffers unauthorised access to customer information

On May 1, Dropbox reported that on April 24, they became aware of unauthorised access to the

Dropbox Sign production environment. Further analysis revealed that a threat actor had accessed Dropbox Sign customer information. `technology`

Dell data breach exposes 49 million customer records through partner portal API
During early May, Dell warned impacted customers following a significant data breach, affecting 49 million customer records. The breach was first disclosed on April 28, when a threat actor named Menelik listed the stolen database for sale, claiming to have exploited a partner portal API, gaining access by registering under fictitious company names without proper verification, and, once inside, scraped various customer purchase information. `technology`

Microsoft faces privacy issues over its new AI-powered Recall feature
On May 21, Microsoft announced its new AI-powered Windows 11 Recall feature which has sparked privacy concerns, with fears it creates new attack vectors for data theft. Recall takes screenshots every few seconds, storing them locally for up to three months, searchable via AI. `artificial intelligence`

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 e-mail. However, they recommend that all users refresh their tokens. `artificial intelligence`

Ticketmaster confirms massive breach after stolen data for sale online
On May 20, Live Nation has 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`

Information operations

Emerald Divide's ongoing influence campaign targeting Israeli audiences
On May 8, Recorded Future reported about an ongoing influence campaign from Iran-linked Emerald Divide (Storm-1364). They exploited the Israel-Hamas conflict to stir dissatisfaction among Israelis about their government's responses. The campaign employs advanced and innovative tactics, including AI-generated deepfakes, digital e-mailing through crowdfunding platforms, social media, and web mapping tools to enhance engagement and impact. `iran`

CopyCop a pro-Russia information operation used generative AI
On May 9, Recorded Future reported that a pro-Russia information operation named CopyCop used generative AI to plagiarise and modify content from legitimate media sources to tailor political messages with specific biases. The information operation in particular targeted audiences in the UK, France and the US. The content disseminated by CopyCop ranged from pro-Russia content about Russia's war on Ukraine to criticism about Israeli military operations in Gaza. `russia` `artificial intelligence`

OpenAI disrupts covert AI-driven influence operations
On May 30, OpenAI reported having halted several covert influence operations exploiting AI for deceptive activities, including Bad Grammar and Doppelganger, two operations originating from Russia. These disruptions, achieved in collaboration with various sectors, targeted operations from Russia, China, and Iran, among others. These efforts aim to enhance transparency and foster

community-wide best practices against the misuse of AI in global influence campaigns. `china` `iran` `russia` `artificial intelligence`

Meta shuts down Facebook network linked to pro-Israel influence campaign
On May 29, Meta announced the removal of numerous Facebook accounts tied to a pro-Israel influence operation. This campaign, also active on X and YouTube, aimed to support Israeli authorities during the war and other related activities. The involved company, STOIC, is based in Tel-Aviv and specialises in online communication campaigns. `israel` `social media`

Hacktivism

Stark Industries Solutions linked to Russian threat actor NoName057
On May 2023, KrebsOnSecurity reported that the Russia-linked Stark Industries Solutions internet hosting firm which emerged as a key player in DDoS attacks on Ukrainian and European entities since 2022. An investigation revealed its use as a global proxy network for concealing cyberattacks. Notably, the pro-Russia group NoName057(16) uses Stark Industries for DDoS attacks and recruiting hacktivists via Telegram. `russia`

Significant vulnerabilities

Zero-day Vulnerability in Chrome
On May 15, 2024, Google has released an advisory addressing nine vulnerabilities, including a new zero-day bug identified as “CVE-2024-4947”. It has been reported that this vulnerability is being actively exploited. This is the seventh zero-day vulnerability fixed by Google this year. See CERT-EU’s SA 2024-044.

Multiple Vulnerabilities in Microsoft Products
On May 16, 2024, Microsoft addressed 61 vulnerabilities in its May 2024 Patch Tuesday update, including two actively exploited zero-days. This Patch Tuesday also fixes one critical vulnerability, a Microsoft SharePoint Server Remote Code Execution Vulnerability. See CERT-EU’s SA 2024-045.

Multiple Vulnerabilities in Git
On May 14, 2024, GitHub announced the release of Git version 2.45.1, addressing three critical vulnerabilities impacting multiple platforms, including Windows, macOS, Linux, and BSD. These vulnerabilities could allow for remote code execution and unauthorised file modifications. See CERT-EU’s SA 2024-046.

Critical Vulnerability in GitHub Enterprise Server
On May 21, 2024, GitHub disclosed a critical vulnerability in GitHub Enterprise Server (GHES) impacting instances using SAML single sign-on (SSO) with encrypted assertions. This vulnerability allows attackers to forge SAML responses, granting unauthorised administrative access without authentication. A proof of concept is publicly available. See CERT-EU’s SA 2024-047.

Critical Vulnerability in Veeam Backup Enterprise Manager
On May 21, 2024, Veeam issued fixes addressing multiple security flaws in Veeam Backup Enterprise Manager, including a critical vulnerability allowing unauthenticated attackers to bypass authentication and gain access to the web interface as any user. See CERT-EU’s SA 2024-048.

Multiple Vulnerabilities in QNAP Products
On May 21, 2024, QNAP released a security advisory addressing multiple flaws, including a zero-day vulnerability in the shared feature of QTS. These vulnerabilities could allow remote attackers to execute arbitrary code. See CERT-EU’s SA 2024-049.

Multiple Vulnerabilities in Ivanti EPMM
On May 15, 2024, Ivanti released a security advisory addressing multiple vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM), formally known as MobileIron. An attacker could exploit these flaws to execute arbitrary commands on the appliance. See CERT-EU's SA 2024-050.

Vulnerabilities in GitLab
On May 22, GitLab has released several versions for GitLab Community Edition (CE) and Enterprise Edition (EE) containing important bug and security fixes. These fixes notably address a vulnerability that would allow an attacker to take accounts over via an XSS vulnerability. See CERT-EU's SA 2024-051.

Vulnerability in Cisco FMC Software
On May 22, Cisco released an advisory regarding an SQL injection vulnerability affecting its Firepower Management Center (FMC) Software. If exploited, this vulnerability could allow an attacker to obtain any data from the database, execute arbitrary commands on the underlying operating system, and elevate privileges to root. See CERT-EU's SA 2024-052.

Zero-day Vulnerability in Check Point Security Gateways
On May 28, 2024, Check Point issued an advisory about a zero-day vulnerability, CVE-2024-24919, affecting Check Point Security Gateways. This high-severity information disclosure vulnerability can be exploited to gain unauthorised access to sensitive information on systems with remote Access VPN or Mobile Access Software Blades enabled. See CERT-EU's SA 2024-053.

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.