Cyber Security Brief (November 2023)

December 1, 2023 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 282 open source reports for this Cyber Security Brief[1].
- Relating to **cyber policy and law enforcement**, the French government has asked ministers to replace third party messaging apps with a secure French app, ENISA has initiated collaboration with Ukraine, and there were various European law enforcement operations against cybercrime. In the rest of the world, India drafted regulations to combat deepfake content, the US CISA and NCSC-UK released guidelines for secure AI development, and on two separate cases of cooperation, South Korea with the US, and Japan with South Korea, and Australia established cooperation on cyber threats.
- On the **cyberespionage** front, likely Russia-linked threat actors engaged in a spearphishing campaign and USB worm spreading. Serbian government critics were targeted by the Pegasus spyware. In the rest of the world a reportedly Chinese threat actor targeted South Pacific entities, there was activity in the Middle East and Israel, a likely North Korean threat actor performed a wide-ranging supply chain attack, and Apple warned Indian opposition leaders and journalists of potential state-sponsored espionage.
- Relating to **cybercrime**, ransomware attacks have affected major companies in the banking, aerospace, automotive, and energy sectors. Alphv filed a SEC complaint against a victim they had breached. In Europe, for November, the top most active ransomware operations have been Lockbit, BlackBasta, 8Base, and Play; the most targeted sectors have been manufacturing, legal & professional services, construction & engineering, transportation, and healthcare.
- As regards **disruptive** incidents, a likely Russia-linked threat actor reportedly targeted Ukraine's energy systems in late 2022, and there were cyber attacks against Denmark's critical infrastructure in May 2023. The Russian Sberbank experienced a powerful DDoS attack, while a cyber attack in Australia disrupted freight movement in ports.
- There were a number **information operations** of likely Russian origin in Europe, and a Chinese influence operation looking to exploit US political divisions.
- Significant **data exposure and leaks** incidents affected organisations in the nuclear research and IT sectors. Ukraine's intelligence service also reportedly hacked Russia's aviation agency.

- On the **hacktivism** front, the Israel-Hamas conflict dominated activities, with pro-Palestine group claims of hacks in France, the UK, India, and Canada. A pro-Russia hacktivist group claimed DDoS attacks on German and Dutch entities and Ukrainian hacktivists exposed illegal Russian trade activities. Notably, Russian media revealed the identity of the alleged leader of the group Killnet.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in November 2023.

Europe

Cyber policy and law enforcement

French government members urged to switch messaging apps *Messaging apps*

According to newspaper Le Point, France's Prime Minister Elisabeth Borne has invited ministers and members of their cabinets to uninstall "any messaging application" such as WhatsApp, Telegram or Messenger, due to cybersecurity concerns. The head of government asked to instead install Olvid, a more secured application developed in France.

Rising Cyber Threats in Germany *Threat assessment*

Germany is currently experiencing a significant increase in cyber threats, notably with an exceptionally high risk of ransomware attacks, according to the November 2 report from the German Federal Office for Information Security (BSI). The threat level is described as the highest ever recorded, with an average of 332.000 new variants of malicious software created per day. Ransomware remains the primary cyber threat, and small to medium-sized enterprises, as well as local administrations, are particularly vulnerable.

Enhanced EU-Ukraine collaboration *Collaboration*

The European Union Agency for Cybersecurity (ENISA) announced on November 13 its collaboration with Ukraine to enhance cybersecurity through the sharing of best practices. The agreement aims to strengthen the European cybersecurity systems and enables Ukraine to contribute to international policies, leveraging its expertise in Russian cyber operations. This cooperation also involves Ukraine adapting to European cybersecurity standards.

Police dismantle ransomware group behind attacks in 71 countries *Law enforcement operation*

Law enforcement agencies from seven countries, working with Europol and Eurojust, have arrested core members of a ransomware group in Ukraine. This group was responsible for attacks on organisations in 71 countries, using ransomware like LockerGoga, MegaCortex, HIVE, and Dharma. The arrested individuals had various roles, including breaching networks and laundering cryptocurrency payments.

Phishing gang dismantled in a joint-operation *Law enforcement operation*

The Czech and Ukrainian police, aided by Europol and Eurojust, dismantled a major phishing gang responsible for defrauding European victims of millions of euros, including over 8 million euros in Czechia. Operating from Ukrainian call centres, the group conducted voice phishing attacks by impersonating bank employees and police officers, tricking victims into transferring funds to their controlled accounts.

Ukraine police disrupt 872.000 US dollars cryptocurrency cybercriminal wallet *Law enforcement operation*
On November 17, Ukraine's police announced the disruption, in coordination with French law enforcement authorities, of a cybercrime group reportedly responsible for stealing nearly 872.000 US dollars from EU citizens across at least 300 websites.

Ukrainian hacker ringleader arrested in global ransomware operation *Law enforcement operation*
A 32-year-old alleged ringleader of a Ukrainian hacker gang specialising in ransomware attacks was arrested on November 28 in a joint operation by US, European, and Ukrainian police. The operation targeted 30 properties in western and central Ukraine, resulting in the apprehension of key figures behind the cybercrime network. Europol coordinated the effort, emphasising the collaboration of authorities between the countries.

Spanish National Police arrest 45 people linked to fraud schemes targeting the elderly *Arrest*
On November 5, the Spanish National Police (Policía Nacional) announced it had detained 45 people impersonating government officials and defrauding elderly people of more than 300.000 euros since at least August 2022. The cybercriminals posed as various officials from Spanish courts, the Treasury, or the Civil Guard and called victims or went to the victims' homes to elicit their banking information.

Cyberespionage

APT29 spearphishing targets European organisations *Russian threat actor*
On November 14, Ukraine's National Cyber Security Coordination Center (NCSCC) reported on a new wide-ranging APT29 spearphishing campaign, which occurred in September 2023. The campaign targeted several entities across Europe including the European Commission, diplomatic bodies (Ministries of Foreign Affairs, embassies), internet service providers (ISP), and international organisations.

Gamaredon USB worm may have spread beyond Ukrainian targets *Russian threat actor*
On November 17, CheckPoint researchers reported on a Russia-linked Gamaredon campaign which spreads the LitterDrifter USB worm. Most of the victims appear to be located in Ukraine, but the USB worm appears to have also spread beyond. CheckPoint identified indications of possible LitterDrifter infections in Poland, Germany, the US, Vietnam, Hong Kong, and Chile.

Appin Security Group's global hack-for-hire operations *PSOA*
SentinelLabs has uncovered the extensive global intrusions by Appin Security Group, a prominent hack-for-hire company, involving espionage and surveillance across multiple countries including Norway, Pakistan, China, and India. Despite public disclosures, the methodologies behind malware creation and network infrastructure by hack-for-hire groups like Appin remain largely obscure, posing a significant challenge for security researchers. Appin, originating in India in 2009, has been influential in shaping the current landscape of private-sector-offensive-actors (PSOA), with their operations impacting global governmental and private entities in various legal disputes.

Serbian government critics targeted with spyware *PSOA*
According to Citizenlab, in 2023, two Serbian government critics were targeted with spyware. Citizen Lab analysed evidence, supported by Access Now and the SHARE Foundation, with Amnesty International confirming. The attacks used iPhone's HomeKit function around August 16, 2023, possibly involving NSO Group's Pegasus spyware, but the exact spyware variant remains unconfirmed due to limited evidence.

Cybercrime

Slovenian power provider hit by ransomware attack *Energy*
Slovenian largest power company, Holding Slovenske Elektrarne (HSE), faced a ransomware attack that encrypted files but didn't disrupt power production. HSE is a critical infrastructure provider in Slovenia, and the attack is attributed to the Rhysida ransomware gang, known for not specifying ransom amounts in their notes.

Ransomware disrupts British Library services *Culture*
The British Library, the national library of the United Kingdom, suffered a ransomware attack, impacting online and onsite services, including Wi-Fi. While internal human resources (HR) data has been leaked, there's no evidence of user data compromise, and the Library took protective measures and investigated the attack with the help of cybersecurity experts and law enforcement.

Disruption

Sandworm disrupts power in Ukraine *Energy*
According to a report release by Mandiant on November 9, the Russia-linked Sandworm threat actor has transitioned to using living-off-the-land (LoL/LOTL) techniques for more efficient breaches of industrial control systems (ICS). The attackers gained access to the operational technology (OT) environment through a MicroSCADA server. They utilised native binaries and lightweight tools to execute their commands, resulting in a power outage.

Danish critical infrastructure targeted *Energy*
On November 12, Sektor-CERT, a Danish incident response organisation, reported that in May 2023, Denmark faced cyber attacks targeting critical infrastructure. The activity exploited vulnerabilities in Zyxel firewalls in 22 companies in the energy sector. Eleven companies were compromised. At least one organisation suffered a disruption of operations as part of the remediation activity.

Hacktivism

Pro-Palestine hacktivist claims website defacements in numerous countries *Israel-Hamas*
On November 2, the pro-Palestine hacktivist entity IRoX Team claimed to have hacked and defaced more than 30 websites belonging to entities based in France, the UK, India, and Canada in response to their support of Israel, amid the ongoing Israel-Hamas conflict.

Pro-Russia hacktivist targets Germany and the Netherlands *Germany, Netherlands*
On November 3, the pro-Russia hacktivist group NoName057(16) (a.k.a. NoName) claimed responsibility for DDoS attacks against several German and Dutch entities across multiple sectors. Telegram posts expressed support for a then striking German trade union and mentioned the Dutch Prime Minister's defence policy coordination visit with Ukrainian Prime Minister.

Information operations

France accuses Russia of 'online interference' *France*
France accused Russia on November 9 of interfering in its internal affairs when the latter shared online photos of Stars of David found painted on dozens of buildings in Paris. The foreign ministry in a statement accused the Russian RRN/Doppelganger network of attempting to "exploit international crises to sow confusion and create tension in the public debate in France and Europe", and of mounting a "new operation of Russian online interference".

French report flags Azeri-linked disinformation campaign targeting 2024 Olympics *France*
France's state service for Vigilance and Protection against Foreign Digital Interference (Viginum) uncovered a disinformation campaign from Azerbaijan aimed at undermining Paris' hosting of the 2024 Olympics. The campaign, which ran on social media, used various methods to damage France's reputation as an Olympic host, including images and videos of clashes with the hashtag #boycottparis2024. The campaign, however, couldn't be directly tied to Azerbaijani authorities.

Russia makes fake Der Spiegel and Fox News websites to spread disinformation *Germany*
In a report published on November 1, Ukraine's Strategic Communications and Information Security Center revealed that Russia had created fake websites that mimicked prominent news organisations such as Der Spiegel and Fox News to spread disinformation. Aspects of the report seem similar to a pro-Russia information operation, publicly referred to as Doppelganger.

Moldova publishes report describing hybrid warfare campaign from Russia *Moldova*
In a report published in early November, Moldovan intelligence agency said they identified a subversive scenario initiated in 2022 by the Russian Federation and criminal groups that aimed at violently overthrowing democratic governance and transferring power to criminal groups. These activities included manipulation, propaganda, cyber attacks, and corruption efforts to influence elections and undermine Moldova's democratic system.

World

Cyber policy and law enforcement

India drafting regulations to combat deepfake content *Regulations*
India is drafting regulations to combat deepfake content, aiming to address the potential negative impact on society. The Deputy IT Minister urged social media platforms to inform users about the prohibition of sharing deepfakes, and all platforms have agreed to align their content guidelines with government regulations.

US CISA and NCSC-UK provide guidelines for developing secure AI systems *Artificial intelligence*
The US CISA and NCSC-UK have released joint guidelines for secure AI system development, endorsed by 23 cybersecurity organisations. These guidelines promote Secure-by-Design principles for all AI systems and are aimed at AI providers while encouraging all stakeholders to use them for informed decision-making.

US, Japan, and South Korea cooperation to address North Korean cyber threats *Cooperation*
On November 6, South Korea, the US, and Japan established a high-level consulting body to address global cyber issues, focusing on the cyber activities of North Korea. They agreed to meet quarterly to discuss cyber threats posed by North Korea. Additionally, on October 30, South Korea and Australia agreed to work together to identify and counter cyber threats, forming a working group to plan their cooperation.

Philippines weighs TikTok ban amid data privacy concerns *Ban*
The Philippine government is forming a task force to consider banning public officials from using TikTok due to espionage concerns. The task force includes agencies like the National Intelligence Coordinating Agency (NICA), and the decision is pending a threat assessment report. The move was prompted by worries about information operations and psychological warfare.

US government sanctions North Korea's Kimsuky hacking group *Sanctions*
On November 30, the US Treasury's OFAC sanctioned the North Korean group Kimsuky for hacking to support the country's strategic goals. They also imposed sanctions on eight North Korean agents for aiding sanctions evasion and WMD programs. These measures were a response to North Korea's alleged satellite launch on November 21, which hindered their income, resources, and WMD program advancement. Kimsuky was previously linked to North Korea's main foreign intelligence service in August 2010.

US sanctions Russian who laundered money for Ryuk ransomware affiliate *Sanctions*
The US Department of the Treasury's Office of Foreign Assets Control (OFAC) has sanctioned Russian national Ekaterina Zhdanova for laundering millions in cryptocurrency for various individuals, including ransomware actors.

Russian FSB arrest two individuals for allegedly supporting pro-Ukraine cyber operations *Arrest*
The Russian FSB arrested two individuals accused of pro-Ukraine cyber attacks on Russian infrastructure. One is a student, the other a 36-year-old man from Russia, claimed to be linked to a Ukrainian cyber unit. They targeted Russian networks, which were supporting hacktivist groups, and attacked critical infrastructure with malware.

Cyberespionage

Mustang Panda targets the Philippines as tensions flare in the South Pacific *Chinese threat actor*
According to a report by PaloAltoNetworks, in August 2023, the likely China-linked Mustang Panda (a.k.a. Stately Taurus) threat actor executed three campaigns targeting entities in the South Pacific including the Philippines government. This coincided with real-world tensions: early August, a Chinese Coast Guard vessel fired its water cannon at a Philippine vessel resupplying the disputed Second Thomas Shoal in the Spratly Islands, leading to increased tensions, subsequent joint patrols with the US, naval exercises with Australia, the termination of a hotline with China, and removal of Chinese barriers near the Scarborough Shoal by the Philippine Coast Guard.

Iranian cyberespionage group Scarred Manticore targets Middle East financial and government sectors *Iranian threat actor*

According to Check Point Research, an ongoing Iranian espionage campaign led by Scarred Manticore, linked to the Ministry of Intelligence and Security (MOIS) is targeting high-profile organisations in the Middle East. Targeted sectors include government, military, and telecommunications, as well as IT service providers, financial institutions, and NGOs. Some tools used in this campaign have also been linked to a MOIS-sponsored attack on Albanian government infrastructure (DEV-0861).

Agonizing Serpens targeting the Israeli higher education and tech sectors *Iranian threat actor*

From January 2023 to October 2023, PaloAltoNetworks researchers investigated cyber attacks targeting Israel's education and technology sectors. The attackers aimed to steal sensitive data and used wipers to cover their tracks. The attacks were linked to an Iranian-backed APT group called Agonizing Serpens (a.k.a. Agrius, BlackShadow, Pink Sandstorm, DEV-0022).

Iran-linked Imperial Kitten threat actor targeting Middle East's tech sectors *Iranian threat actor*

According to Crowdstrike, in October 2023, the Iran-linked threat actor they track as Imperial Kitten, used watering-hole attacks to target the transportation, logistics, and technology sectors in the Middle East. Reportedly, the adversary, active since at least 2017, likely fulfils Iranian strategic intelligence requirements associated with IRGC operations.

North-Korea linked threat actor conducted a supply-chain attack on a software company. *North-Korean threat actor*

Microsoft Threat Intelligence identified a supply-chain attack by North Korea's Diamond Sleet, involving a tampered CyberLink application installer with a malicious payload, impacting over 100 devices globally. The attack, attributed with high confidence to Diamond Sleet, features a second-stage payload communicating with previously compromised infrastructure and targets various sectors including IT, defence, and media.

UK and South Korea: Hackers use zero-day in supply chain attack *North Korean threat actor*

NCSC UK and South Korea's National Intelligence Service (NIS) issued a warning about the North Korean Lazarus hacking group. They report that Lazarus is exploiting a zero-day vulnerability in the MagicLine4NX software, developed by Dream Security in South Korea. This breach is being used for supply-chain attacks, targeting companies using this software for secure logins.

Apple alerts Indian Opposition leaders to state-sponsored iPhone threats *Unattributed threat actor*

Apple has issued warnings to Indian opposition leaders and journalists about potential state-sponsored iPhone attacks, though it has not attributed the actions to a specific threat actor. While India's IT Minister is investigating the matter, concerns persist about the government's use of spyware on opposition figures, emphasising the need for transparency and analysis regarding spyware purchases and deployments by the Indian government.

Cybercrime

World's largest commercial bank ICBC confirms ransomware attack *Bank*

ICBC, the Industrial & Commercial Bank of China, experienced a ransomware attack on November 8, disrupting its financial services systems. However, it quickly isolated the affected systems, reported the incident to law enforcement, and is working to recover. The attack affected the US Treasury market but didn't impact other ICBC systems or its New York Branch.

LockBit ransomware leaks gigabytes of Boeing data *Aerospace*
The LockBit ransomware group disclosed that it stole and leaked gigabytes of data from Boeing, a major aerospace company that specialises in commercial aircraft and defence contracting. Boeing has confirmed the cyber attack and is currently assessing the extent of the breach.

Qilin ransomware claims attack on automotive giant Yanfeng *Automotive*
The Qilin ransomware group claimed responsibility for a cyber attack on Yanfeng Automotive Interiors (Yanfeng), one of the world's largest automotive parts suppliers. Yanfeng is a Chinese automotive parts developer and manufacturer focused on interior components and employs over 57.000 people in 240 locations worldwide.

Ransomware attack prompts US hospital chain to divert some emergency room patients elsewhere *Health*
A ransomware attack on Ardent Health Services, a healthcare chain with 30 hospitals in six states, has led to the diversion of patients from some of its emergency rooms to other hospitals. The attack occurred on November 23, prompting Ardent Health Services to take its network offline and suspend user access to IT applications used for patient care documentation and certain elective procedures.

Alphv / BlackCat ransomware files SEC complain over victim's failure to disclose data breach *Ransomware*
Ransomware group Alphv / BlackCat has breached MeridianLink, a California-based company. They're claiming to have filed a complaint with the SEC, accusing MeridianLink of not disclosing the breach within the required four business days, as per SEC rules announced in July. This complaint is being used to pressure the company into meeting their ransom demands.

Google sues to block AI ads preying on small businesses *Artificial intelligence*
According to an article by the Wall Street Journal, scammers in India and Vietnam use fake Facebook ads to deceive US small businesses into downloading Google's non-downloadable Bard AI chatbot. Google filed a lawsuit against these scammers, aiming to stop their actions and claim damages. It's the first lawsuit of its kind for a major tech company's AI product. Scammers operate via fake accounts like Google AI.

Data exposure and leaks

Data breach on Idaho National Laboratory *Nuclear research*
The Idaho National Laboratory, a major US nuclear research centre, has experienced a cyber attack, confirmed following the online leak of human resources data by 'SiegedSec' hacktivists. The facility, spanning 890 square miles and housing 50 experimental nuclear reactors, is integral to atomic energy and national security research, employing over 5.700 specialists.

Software provider data breach exposes millions of records *IT*
TmaxSoft, a Korean IT company, inadvertently exposed over 50 million sensitive records through a 2 TB Kibana dashboard, which remained accessible for more than two years. Cybersecurity researchers first identified this breach in January 2023, tracing its origin back to June 2021.

Ukraine says it hacked Russian aviation agency, leaks data *Aviation*
Ukraine's intelligence service says it hacked Russia's aviation agency, Rosaviatsia, to expose problems in Russia's aviation sector, including issues caused by sanctions and inadequate plane maintenance.

Disruption

Russian bank hit by DDoS *Bank*
On November 8, Russian financial organisation Sberbank announced in a press release that two weeks before it faced the most powerful DDoS attack in recent history. Sberbank is a majority state-owned banking and financial services company and the largest institute in Russia, holding about a third of all assets in the country. Following Russia's invasion of Ukraine, the bank faced international blockades and sanctions and was the target of west-aligned hacktivists multiple times.

Cyber attack blocks Australian ports *Logistics*
In a media statement, international logistics firm DP World Australia announced that a cyber attack severely disrupted the regular freight movement in multiple large Australian ports. DP World has an annual revenue of over 10 billion US dollars and specialises in cargo logistics, port terminal operations, maritime services, and free trade zones. It is responsible for operating 82 marine and inland terminals in 40 countries.

Hacktivism

Ukrainian hacktivist targets Russian Ministry of Defence *Russia*
On November 27, the pro-Ukraine hacktivist entity Kiber Sprotyv (Cyber Resistance) claimed, on their Telegram chan, a hack-and-leak operation affecting the Department of Information and Mass Communications of the Russian Ministry of Defence

Ukrainian hacktivist exposes Russian airlift operations *Russia*
Ukrainian hacktivist group Cyber Resistance provided InformNapalm, a volunteer intelligence community, with data from the mailbox of Maxim Okss, a pilot associated with the sanctioned Aviacon Zitotrans airline. This data uncovers the involvement of Russian airlines in transporting weapons, ammunition, and sanctioned goods from Iran, South Africa, and Mali to Russia.

Killnet's alleged leader's identity revealed *Doxxing*
Russian state media revealed, on November 27, the identity of the alleged leader of the pro-Russia hacktivist group Killnet, known as "Killmilk", raising questions about the extent of cooperation or tolerance of such actors by the Russian state. The case also highlights the internal conflicts within the cybercrime/hacktivism underworld.

Information operations

Meta says it broke up Chinese influence operation looking to exploit US political divisions *Chinese infoops*
Meta disclosed on November 30 that it has removed five separate Chinese networks targeting foreign audiences this year, marking a notable escalation compared to previous years when only two such networks were removed between 2017 and November 2020. One of the recently taken-down networks included nearly 5.000 fake accounts and primarily focused on Americans, posting about US politics and US-China relations.

Significant vulnerabilities

Critical Vulnerabilities in Veeam ONE — *Veeam ONE*
On November 6, Veeam has released an advisory addressing critical vulnerabilities affecting the Veeam ONE product. These vulnerabilities could allow an attacker to steal NTLM hashes, or to achieve Remote Code Execution. Veeam has released hotfixes for these vulnerabilities, and it is recommended applying them as soon as possible. See CERT-EU's SA 2023-086.

Critical Vulnerabilities in QNAP products — *QNAP*
On November 4, QNAP Systems has released advisories addressing critical vulnerabilities affecting multiple versions of the QTS operating system and applications on its network-attached storage (NAS) devices. These vulnerabilities could allow an attacker to achieve Remote Code Execution. It is recommended updating affected devices as soon as possible. See CERT-EU's SA 2023-087.

High Vulnerabilities in Ivanti Endpoint Manager Mobile — *Ivanti Endpoint Manager Mobile*
On November 9, Ivanti disclosed two vulnerabilities, "CVE-2023-39335" and "CVE-2023-39337", affecting all versions of Endpoint Manager Mobile (formerly MobileIron Core). The vulnerabilities can be chained to allow an unauthenticated user to access resources behind Sentry. See CERT-EU's SA 2023-088.

VMware Cloud Director Critical Vulnerability — *VMware*
On November 14, VMware issued an advisory about a critical authentication bypass vulnerability, "CVE-2023-34060", affecting Cloud Director Appliance. The CVSSv3 score is 9.8, indicating a critical level of severity. This vulnerability is present on an upgraded version of VMware Cloud Director Appliance. See CERT-EU's SA 2023-089.

Microsoft Software Critical Zero-Day Vulnerabilities — *Microsoft*
On November 15, 2023, Microsoft released patches for 63 security flaws in its software, including five new zero-day vulnerabilities, three of which are actively exploited. These vulnerabilities pose significant risks and require immediate attention. See CERT-EU's SA 2023-090.

High Vulnerabilities in Citrix Hypervisor — *Citrix Hypervisor*
On November 15, 2023, Citrix issued an advisory regarding two vulnerabilities affecting Citrix Hypervisor 8.2 CU1 LTSR that could allow malicious code in a guest VM to compromise the host. See CERT-EU's SA 2023-091.

Critical vulnerability in FortiSIEM — *FortiSIEM*
On November 14, Fortinet released an advisory regarding a critical vulnerability affecting FortiSIEM which may allow a remote unauthenticated attacker to execute unauthorised commands via crafted API requests. See CERT-EU's SA 2023-092.

High Vulnerabilities in Google Chrome — *Google Chrome*
On November 28, Google has released an emergency security update to address six high vulnerabilities found in Chrome. Google is aware that an exploit exists for one of the vulnerabilities, tracked as "CVE-2023-6345". See CERT-EU's SA 2023-093.

All CERT-EU's Security Advisories are available to the public on CERT-EU's website, `https://www.cert.europa.eu/publications/security-advisories#2023`

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.