CERT-EU

Cyber Security Brief (August 2023)

September 1, 2023 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 233 open source reports for this Cyber Security Brief[1].
- Relating to **cyber policy and law enforcement**, major online platforms in the EU must now comply with the Digital Services Act's regulations, including annual assessments and algorithm safety for minors. Meanwhile, law enforcement efforts have disrupted cybercrime operations. In the rest of the world, China is tightening rules on facial recognition, while the US enhances AI cybersecurity efforts and updates national cybersecurity frameworks. Apple faces fines in Russia and Meta disrupted a Chinese information operation.
- On the **cyberespionage** front, recent cybersecurity events in Europe involved incidents in which Ukrainian forces thwarted a cyber operation by Russian military intelligence, while North Korean hackers exploited Zoho software vulnerabilities against the US and UK infrastructure. A new cyberespionage group, MustachedBouncer, targeted foreign embassies in Belarus using advanced tactics and malware. In the rest of the world, various cyber threat actors have escalated global attacks, with entities linked to China and Russia targeting institutions across sectors and regions. Vulnerabilities such as the "Downfall" attack on Intel microprocessors expose sensitive data.
- Relating to **cybercrime**, Finland has experienced a fourfold increase in ransomware attacks since its NATO application, hosting providers in Denmark and the German Federal Bar Association faced ransomware attacks, with significant data losses and disruptions reported. Notably, the ransomware group LockBit faces potential decline due to operational issues. In Europe, for August, the top most active ransomware operations have been Lockbit, Cloak, AlphV, and METAENCRYPTOR; the most targeted sectors have been manufacturing, legal and professional services, construction and engineering, technology, and government.
- Regarding **data exposure and leaks**, the personal data of police officers in Northern Ireland and London were compromised due to various lapses. Additionally, France's unemployment agency and the UK Electoral Commission experienced breaches, exposing personal data of millions of individuals. Worldwide, breaches via the MOVEit software continued to have a significant impact to businesses.

- On the **hacktivism** front, in August, the pro-Russia hacktivist group Noname056 launched a series of DDoS attacks against entities in several European countries, reacting to their political stances on Ukraine. Meanwhile, SiegedSec made claims of breaches in Romanian and Pakistani organisations.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in August 2023.

Europe

Cyber policy and law enforcement

The EU examines the impact of social media in society *Regulation*

The EU's Digital Services Act (DSA) mandates that major online platforms with over 45 million users in the European Union, including Instagram, Snapchat, TikTok, Pinterest, and YouTube must comply with extensive rules by the end of August. The platforms must provide their first yearly assessment of how their design, algorithms, advertising, and terms of service impact societal issues, proposing and implementing measures under scrutiny. Regulations include preventing algorithms from recommending harmful content to minors.

Qakbot malware infrastructure takedown *Takedown*

On August 30, Europol and Eurojust announced they had supported the coordination of a large-scale international operation that has taken down the infrastructure of the Qakbot malware. The operation also led to the seizure of nearly 8 million Euros in cryptocurrencies. The operation involved judicial and law enforcement authorities from France, Germany, Latvia, The Netherlands, Romania, the UK and the US. Qakbot, operated by a group of organised cybercriminals, targeted organisations across multiple countries, stealing financial data and login credentials. Cybercriminals used this persistent malware to commit ransomware, fraud, and other cyber-enabled crimes.

Hosting provider of illicit material taken down *Takedown*

Authorities from the US and Poland have collaborated to shut down the well-known "bulletproof" (very permissive to the content allowed) hosting platform Lolek Hosted, which was being used by cybercriminals for malicious activities. Bulletproof hosting providers offer anonymity to hackers and are commonly used for distributing malware and supporting cyberattacks.

London jury convicts two Lapsus$ operators *Sentence*

A London jury convicted two members of the Lapsus$ Group for their roles in multiple data theft-and-leak operations. Lapsus$ is a group that has conducted data theft extortion operations since mid-2021. They are motivated by both financial gain and a desire for notoriety. Arion Kurtaj, an 18-year-old operator, was found guilty of various offences, and an unnamed 17-year-old operator was found guilty of fraud, blackmail, and a Computer Misuse Act offence.

Cyberespionage

Ukraine thwarted a Russian cyber operation

Russian threat actors

On August 8, the Security Service of Ukraine (SBU) and the Armed Forces of Ukraine announced they had successfully thwarted a cyber operation conducted by Russian military intelligence (GRU) aimed at infiltrating the Defence Forces of Ukraine. The GRU's cyber units reportedly attempted to launch extensive cyber attacks to gain control over Android devices of Ukrainian military personnel, which were used for planning and performing combat missions. The SBU identified and neutralised various malware instances deployed by Russian cyber intelligence, particularly the Sandworm hacker group from military unit 74455. The attack exploited captured battlefield devices to gain access to local networks using stolen keys and employed Android Debug Bridge (adb) for installing malicious files on compromised devices.

Lazarus hackers exploit Zoho's ManageEngine vulnerability

North Korean threat actor

North Korean state-backed hacker group Lazarus has been exploiting a critical vulnerability in Zoho's ManageEngine ServiceDesk (CVE-2022-47966) to compromise an internet backbone infrastructure provider and healthcare organisations in the US and UK. The attacks, which began earlier this year, involve deploying the QuiteRAT malware and a new remote access trojan (RAT) called CollectionRAT, with Lazarus displaying evolving tactics such as the incorporation of the Microsoft Foundation Class framework to evade detection and enhance its capabilities.

Cyberespionage group targets foreign embassies in Belarus with local ISP assistance

Unattributed threat actors

According to cybersecurity company ESET, a recently discovered cyberespionage group named MustachedBouncer has been targeting foreign embassies in Belarus, often collaborating with local internet service providers (ISPs). The group, operating since 2014, has compromised embassy staff from various countries, and it employs tactics such as lawful interception systems, including possible use of Russian SORM network interception technology, and custom malware called Disco. ESET suggests that the group cooperates closely with a suspected Belarusian pro-Russian cyberespionage effort named Winter Vivern.

Cybercrime

Increase in ransomware attacks on Finnish organisations linked to geopolitical factors

Multiple sectors

According to Finland's National Cyber Security Centre (NCSC-FI), ransomware attacks on Finnish organisations have quadrupled since Finland applied to join NATO, which the NCSC-FI deputy director general believes could be linked to geopolitical factors. While there has been an increase in cyber incidents, particularly ransomware cases, there hasn't been any publicly visible disruption, thanks in part to the preparedness of Finnish organisations.

Faust ransomware compromised two Danish hosting providers, affecting all of their customers data

Web hosting

On August 18, the Faust ransomware operation targeted two Danish hosting providers (CloudNordic and Azero). Both providers stated that the cybercriminals gained access to the central administration system and the backup systems before deploying the ransomware, encrypting all servers disks, as well as the primary and secondary backup systems. The providers immediately informed their customers that all of their data is lost.

German Federal Bar Association hit by ransomware *Legal*

The German Federal Bar (BRAK) Association discovered on August 2 that it's Brussels' office was hit by a ransomware attack. BRAK is an umbrella organisation overseeing 28 regional bars across Germany and representing about 166.000 lawyers nationally and internationally. The NoEscape ransomware group claimed responsibility for the cyberattack.

Disruption

Regional health service in Madeira faces deliberate cyberattack, suspends non-urgent activities *Health*

On August 7, the Regional Health Service of the Autonomous Region of Madeira, SESARAM, confirmed a deliberate cyberattack aimed at disrupting its normal functioning. As a result, non-urgent clinical activities were suspended, and authorities started collaborating to investigate the attack's origins and impact.

Hacktivist group Solntsepek claims to disable Ukraine's strategic electronic intelligence system *Intelligence*

The hacktivist group Solntsepek claimed responsibility for destroying the strategic electronic intelligence system of the Ukrainian Ministry of Defence's Main Intelligence Directorate. They alleged to have disabled radio reconnaissance posts and satellite communication lines, causing serious damage to the Ukrainian armed forces and paralysing equipment supplied by allies such as the UK and Poland. The group posted materials from the internal network as confirmation, but the extent of the impact remains unverified.

Sabotage activity on Poland's train rail system *Transport*

On August 25, over 20 Polish trains were halted by what was initially reported as a sophisticated cyberattack, seemingly carried out in support of Russia with interludes of the Russian national anthem and excerpts from Putin's speech. The railway system in Poland has been instrumental in delivering aid to Ukraine in the face of Russia's invasion. However, a cybersecurity researcher suggested the disruption may not have been a sophisticated but rather a simple exploit of the trains unencrypted radio system, with a simple "radio-stop" command anyone could broadcast with $30 in equipment.

Hacktivism

Pro-Russia hacktivist group claims DDoS against Italian banks *Italy*

On August 1, Noname056, a pro-Russia hacktivist group, claimed responsibility for a DDoS attack against five Italian financial institutions and eight Italian transportation companies.

Pro-Russia hacktivist group targets Spanish websites *Spain*

On August 4, Spanish news websites reported Spain had endured a forceful two-week campaign of DDoS attacks by Noname056, reportedly in retaliation to Prime Minister Pedro Sánchez's pledge of support for Ukraine's president. The coordinated campaign targeted institutions, banks, media, and more. Russian secret services also allegedly aimed to exploit Spain's post-election uncertainty by suggesting an impending "period of political chaos".

Pro-Russia hacktivist group claims DDoS attacks on Netherlands, Denmark, and Greece

Netherlands, Denmark, Greece

NoName056 claimed to have conducted DDoS attacks against websites in the Netherlands and Denmark from August 21 to 22, 2023, possibly in response to these countries' military aid to Ukraine. The group later announced DDoS activity against Greek public sector transportation entities following Ukraine's announcement of fighter-pilot training in Greece.

Hacktivist group SiegedSec claims breach of a Romanian government entity and a Pakistani bank

Romania

On August 18, hacktivist group SiegedSec claimed to have breached a Romanian government entity and a Pakistani bank, leaking user data from both. They provided a link to a CSV file with the alleged stolen data, as well as announcing their access to unspecified Romanian global navigation satellite system (GNSS) receivers and industrial control systems (ICS). The group also established an account on blackforums.net for sharing leaks and solicited donations in Bitcoin and Monero. The validity of the claims and the data's accuracy cannot be confirmed, and no confirmation of the breaches has been provided by the targeted organisations.

Information operations

Russian hackers employ disinformation to target NATO's Vilnius Summit

NATO

On August 21, social media research firm Graphika revealed that Russian hackers targeted NATO's Vilnius summit, held July 11-12, with disinformation campaigns. The hackers spread fake NATO press releases and purported intelligence documents through web pages and fake social media accounts, attempting to disrupt the summit and sow discord among NATO members while undermining support for Ukraine in its ongoing conflict with Russia.

Data exposure and leaks

Accidental data breach exposes personal details of Northern Ireland police officers

Police

The accidental publication of personal details of police officers and staff in Northern Ireland, including their names, ranks, locations, and roles, occurred due to a data breach resulting from a Freedom of Information (FoI) request. The breach raised concerns about security protocols and data protection practices within the Police Service of Northern Ireland (PSNI).

London Police data breach affects 47.000 officers

Police

On August 26, the London Metropolitan Police announced a breach compromising 47.000 officers' personal details due to a third-party vendor leak. The data included names, ranks, photos, vetting levels, and payroll numbers, with some reports suggesting that counterterrorism and Royal Family protection officers were affected; however, addresses, phone numbers, and financial details were not exposed.

Data breach at Pôle Emploi affecting approximately 10 million people

Employment

Pôle emploi, France's unemployment agency, announced a data breach potentially exposing the personal data of job seekers. While the exact number hasn't been specified by the agency, reports from Le Parisien estimate around 10 million individuals are affected.

Massive data breach exposes UK voter information
The UK Electoral Commission has revealed a significant data breach affecting individuals who registered to vote in the UK between 2014 and 2022. The breach, which was detected in October 2022, with threat actors gaining access in August 2021, exposed personal data, raising concerns about delayed disclosure and potential phishing risks for affected individuals.

Citizens

World

Cyber policy and law enforcement

China drafts rules to restrict and regulate facial recognition technology use
China's Cyberspace Administration is seeking public input on draft rules that tighten the use of facial recognition technology, allowing it for national security purposes while aiming to protect individual rights and safety. The rules prohibit misuse in public spaces, require registration for entities using the technology, and limit its use to specific conditions.

Facial recognition

US administration launches AI cyber challenge to enhance critical software security
The US administration has initiated a two-year competition called the "AI Cyber Challenge" (AIxCC), partnering with AI companies such as Anthropic, Google, Microsoft, and OpenAI, to utilise artificial intelligence to enhance the security of critical software in the US, including software that supports the internet and vital infrastructure. Led by DARPA, the competition aims to identify and address software vulnerabilities using AI, offering nearly 20 million US dollars in prizes and involving a variety of AI technologies to improve cybersecurity.

Artificial intelligence

NIST introduces draft of Cybersecurity Framework 2.0 with expanded scope and new 'Govern' function
The National Institute of Standards and Technology (NIST) has released a draft version of the Cybersecurity Framework (CSF) 2.0, aimed at helping organisations understand, reduce, and communicate cybersecurity risks. The draft includes a new "govern" function, expanding the framework's scope to cover all organisations regardless of type or size, and emphasises cybersecurity as a significant enterprise risk alongside legal and financial risks.

Standard

CISA unveils its cybersecurity strategic plan FY2024-2026
On August 4, the US Cybersecurity and Infrastructure Security Agency (CISA) introduced a strategic plan for the next three years, emphasising three primary objectives: tackling immediate cyber threats, enhancing overall security measures, and promoting widespread security adoption. The plan outlines efforts to establish a future with reduced cyberattacks, resilient organisations, and secure technology frameworks. The goals encompass improving threat visibility, mitigating vulnerabilities, fortifying security practices, advancing cybersecurity investments, and fostering collaboration across government, industry, and global defenders to ensure a secure cyber landscape.

Strategy

Russia fines Apple for not deleting "inaccurate" content on Ukraine conflict
According to Russian news agencies TASS and Interfax, Moscow Court fined Apple 400.000 roubles for not deleting "inaccurate" content about what Russia calls a "special military operation" in Ukraine on apps and podcasts.

Fine

Interpol shuts down 16shop phishing-as-a-service platform, arrests operator and facilitators *Takedown*

Interpol, along with cybersecurity firms and cooperation from private sector partners, has taken down the phishing-as-a-service platform 16shop, resulting in the arrest of the platform operator and facilitators in Indonesia and Japan. The platform offered phishing kits targeting prominent brands and was responsible for creating around 150.000 phishing pages that compromised at least 70.000 users across 43 countries, with stolen data including personal details, account information, and credit card numbers.

Chinese information operation disrupted *Takedown*

Meta disrupted a suspected Chinese information operation named Spamoflauge, which targeted countries including the US, Australia, Japan, the United Kingdom, and Taiwan, promoting Chinese government interests and maligning its perceived adversaries. The operation, notable for its extensive cross-platform reach, transitioned to smaller forums post-detection and reportedly had connections to troll farms in Vietnam, Bangladesh, and Brazil.

A world’s top cybercrime gang has been unmasked *Investigation*

On August 30, WIRED released an article detailing their investigation into documents that expose the inner workings of the Trickbot ransomware gang. The revelation includes the identity of a key member of the group.

Cyberespionage

New China-linked espionage-focused threat actor has emerged and is using stealthy techniques *Chinese threat actor*

Microsoft has identified a new threat actor which it refers to as Flax Typhoon. This group primarily targets government bodies, educational institutions, critical manufacturing, and IT organisations, presumably for espionage activities. Instead of heavily depending on malware to access and sustain presence in a victim’s network, the threat actor leans towards using existing components of the operating system—often referred to as “living-off-the-land binaries” or LOLBins and authorised software.

Suspected Chinese threat actors target Barracuda Systems *Chinese threat actor*

According to cybersecurity firm Mandiant, suspected Chinese threat actors launched a campaign exploiting a Barracuda e-mail security gateway zero day, primarily targeting government entities in the US. Nearly a third of the breaches related to this campaign occurred during October-December 2022 and impacted government agencies.

Attack on Japan’s Cyber Security Agency *Chinese threat actor*

The Financial Times reported on August 29 on the discovery of a breach in the systems of Japan’s National Center of Incident Readiness and Strategy for Cybersecurity (NISC), the organisation responsible for the country’s national defence against cyber attacks. According to both government and private sector sources referenced in the FT article, it is believed that highly likely state-backed hackers were behind the attack, probably supported by China. From their side, Chinese authorities pointed to the possibility of US activity citing past such espionage activity which had become known via the WikiLeaks documents.

China-linked hackers conduct cyber attacks in 17 countries over 3-year campaign *Chinese threat actor*

According to cybersecurity firm Recorded Future, China-linked hackers, attributed to a group named RedHotel, have conducted cyber attacks in 17 countries across Asia, Europe, and North America between 2021 and 2023, targeting sectors such as academia, aerospace, government, media, and research. The group, associated with China’s Ministry of State Security, has been engaged in intelligence gathering and economic espionage, using a variety of offensive tools and a multi-tiered infrastructure for their operations.

APT Group Bronze Starlight exploits VPN provider’s certificate to sign malware for Southeast Asian targets

Chinese threat actor

The China-linked APT group ‘Bronze Starlight’ used a valid certificate belonging to the Ivacy VPN provider’s parent company, PMG PTE LTD, to sign malware aimed at the Southeast Asian gambling industry. This allowed them to evade security measures and appear as legitimate software, with concerns raised over potential data breach at the VPN provider; the certificate was eventually revoked by DigiCert in June 2023.

Russian APT29 targets organisations via Microsoft Teams phishing

Russian threat actor

According to Microsoft, APT29 (aka Midnight Blizzard, Cozy Bear), a hacking group linked to Russia’s Foreign Intelligence Service (SVR), conducted targeted phishing attacks through Microsoft Teams, impacting dozens of global organisations, including government agencies. Using compromised Microsoft 365 tenants, the attackers created technical support-themed domains and sent deceptive messages to trick users into approving multifactor authentication (MFA) prompts, with the ultimate aim of stealing their credentials. Microsoft successfully blocked the threat group and is actively working to mitigate the campaign’s impact.

Iran-run ISP Cloudzy supports nation-state and cybercrime threat actors

Iranian threat actor

Researchers at cybersecurity firm Halcyon discovered that an Iranian-run internet service provider (ISP) called Cloudzy has been supporting more than 20 hacking groups, including state-sponsored threat actors, by providing command-and-control services while representing itself as a legal business.

North Korea is stealing information on Russian missiles

North Korean threat actor

Despite the appearance of a strong alliance between North Korea and Russia since the start of the war in Ukraine, cyber security firm SentinelOne published on August 7 that North Korea is actually targeting Russia in cyberspace to steal information about its missiles. North Korean hacker groups ScarCruft and Lazarus infiltrated NPO Mashinostroyeniya, a Russian company specialising in missiles.

Intel CPUs vulnerable to “Downfall” attack

Intel

A new CPU attack named “Downfall”, which is affecting various Intel microprocessor families has been discovered, enabling attackers to steal sensitive data, passwords, encryption keys, and more from users sharing the same computer. The vulnerability, tracked as CVE-2022-40982, exploits the “gather” instruction in Intel processors, allowing attackers to leak the content of internal vector register files.

Chinese APT targets multiple countries with trojanized applications

Chinese threat actor

A Chinese hacking group, GREF, uploaded spyware-laden Signal and Telegram apps to Google Play and Samsung Galaxy Store, targeting users in multiple countries including Ukraine, the US, and Germany. The BadBazaar spyware embedded in these apps can, among other malicious functions, track device locations, steal call logs and SMS, record phone calls, and access files.

Cybercrime

Threat actor phishing evades anti-phishing by exploiting an e-mail service vulnerability

Marketing

On August 2, security researchers at Guardio’s Research Lab reported detecting a phishing campaign which evaded anti-spam and phishing mechanisms by exploiting a vulnerability in Salesforce e-mail services. The exploited vulnerability allowed the threat actor to craft e-mails under the Salesforce domain and infrastructure. On July 28 the vulnerability was resolved.

A new variant of NodeStealer targets Facebook business accounts

Facebook

Palo Alto Networks' Unit 42 uncovered a Python variant of the NodeStealer malware used in a phishing campaign aimed at Facebook business accounts and cryptocurrency wallets since December 2022. The malware is capable of stealing information from various web browsers such as Google Chrome, Microsoft Edge, Brave, and Opera, that can be used for further attacks. This second variant supports additional features, such as parsing e-mails from Microsoft Outlook, data exfiltration via Telegram, taking over the Facebook account, and anti-analysis capabilities. Meta suspects NodeStealer to originate from threat actors based in Vietnam.

Rising hacker exploitation of Cloudflare Tunnels for covert connections and persistent access

Cloudflare Tunnels

Hackers are increasingly misusing Cloudflare Tunnels, a legitimate feature, to establish concealed HTTPS connections from compromised devices, evade firewalls, and maintain prolonged unauthorised access. This method has gained traction among threat actors, with GuidePoint's recent report noting an uptick in such activity, allowing them to discreetly control compromised services and manipulate connections for stealthy data exfiltration and remote access.

EvilProxy phishing platform targets MFA-protected Microsoft 365 accounts

EvilProxy

The EvilProxy phishing platform has gained prominence for targeting multi-factor authentication (MFA) protected Microsoft 365 accounts. Researchers have identified a surge in successful cloud account takeovers over the past five months, primarily impacting high-ranking executives, with EvilProxy combining brand impersonation, bot detection evasion, and open redirections in its attacks.

Lockbit facing challenges due to rapid growth

Ransomware practices

A report by a security researcher in August revealed that the LockBit ransomware-as-a-service operation, known for its growth, is now facing challenges due to its rapid expansion. The group's affiliates doubled over the past year, causing issues related to customer service response time, failure to release data from non-paying victims, and a delay in delivering a major version. The report suggested that LockBit might not survive beyond 2023 due to these internal issues and the departure of affiliates.

Phishing campaign employing QR codes

Attack techniques

A phishing campaign employing QR codes has been reported by Cofense, on August 16, targeting Microsoft credentials across various industries since May 2023. Notably, a major US Energy company was the primary target. The majority of the links included in the phishing e-mails in which Bing redirects URLs; other domains were associated with the Salesforce application and Cloudflare's Web3 services. QR codes with malicious artefacts can reach inboxes and the malicious link is hidden.

Data exposure and leaks

Massive data breach via MOVEit software affects 600 organisations worldwide

MOVEit

A breach tied to a US software provider has impacted around 600 organisations worldwide, exposing data of approximately 40 million people through the compromised MOVEit Transfer file management program. The group “cl0p” responsible for the breach has escalated its data exposure efforts, sparking concerns about the delayed reporting and the potential for future cyber threats.

Significant vulnerabilities

Critical Vulnerability in Endpoint Manager Mobile *MobileIron*
On August 2, Ivanti disclosed a Remote Unauthenticated API Access Vulnerability affecting EPMM (MobileIron Core) running outdated versions (11.2 and below). On August 7, Ivanti added more recent and supported versions on the list of affected products. The vulnerability tracked as CVE-2023-35082 with as CVSS score of 10 out of 10, is actively exploited and allows an unauthorised, remote actor to potentially access users personally identifiable information and make limited changes to the server. Ivanti has released security patches addressing this vulnerability. This vulnerability is different from CVE-2023-35078. See CERT-EU's SA 2023-056.

Microsoft August 2023 Patch Tuesday *Microsoft*
Microsoft has released its August 2023 Patch Tuesday Security Updates, addressing a total of 74 Microsoft CVEs, including two actively exploited zero-day vulnerabilities, and six Critical vulnerabilities. See CERT-EU's SA 2023-057.

Critical Vulnerability in MobileIron Sentry *MobileIron*
On July 24, 2023, Ivanti published a security advisory about a vulnerability discovered in Ivanti Sentry, formerly known as MobileIron Sentry. The vulnerability tracked as CVE-2023-38035 is an API authentication bypass being exploited in the wild. A successful exploitation allows an attacker to change configuration, run system commands, or write files onto systems. While the CVSS score is high (9.8), the software company assessed as a low risk of exploitation for customers who do not expose 8443 to the internet. See CERT-EU's SA 2023-058.

Multiple Junos OS Vulnerabilities *Junos OS*
Juniper Networks has released fixes to address several vulnerabilities. These vulnerabilities could potentially be chained together to allow unauthorised remote code execution (RCE) on SRX and EX series devices. The combined CVSS score for these flaws is 9.8 (Critical) and a PoC exploit has been publicly released. Therefore, CERT-EU strongly advises users to promptly update their devices to the latest versions, or apply the provided workaround. See CERT-EU's SA 2023-059.

Critical Vulnerability in VMware Aria Operations for Networks *VMware Aria Operations for Networks*
On August 29, VMware released security updates to patch one critical (CVE-2023-34039) and one high-severity (CVE-2023-20890) vulnerability in Aria Operations for Networks, its enterprise network monitoring tool. The flaws were responsibly reported to the vendor and as of the time of writing, there is no evidence of exploitation in the wild. CERT-EU urges users to promptly apply the provided fixes. See CERT-EU's SA 2023-060.

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.