Cyber Security Brief (October 2023)

November 3, 2023 - Version: 1.1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 287 open source reports for this Cyber Security Brief[1].
- Relating to **cyber policy and law enforcement**, European Commissioner Thierry Breton warned Meta and TikTok to address illegal content and disinformation about the Israel-Hamas conflict within 24 hours or face penalties under the EU's Digital Services Act, a multinational law enforcement operation targeted the Ragnar Locker ransomware group, and the US SEC charged SolarWinds' CISO with fraud for misrepresenting cybersecurity practices during the December 2020 cyberattack.
- On the **cyberespionage** front, Vietnam's Ministry of Public Security was accused of using Predator spyware to target officials and journalists, the French national cyber security agency published a report detailing techniques used by the Russia-linked APT28 threat actor, and there were multiple reports on threat actors allegedly originating from North Korea, China, Russia, Belarus and Palestinian territories.
- Relating to **cybercrime**, despite the takedown of the Qakbot malware infrastructure in August, hackers targeted new victims with this malware strain. In Europe, for October, the top five most active ransomware operations have been Lockbit, Medusalocker, Noescape, Play, and Blackbasta; the most targeted sectors have been manufacturing, legal & professional services, retail, construction & engineering, education and healthcare.
- As regards **disruptive** incidents, the telecommunications sector was particularly affected with an undersea communications cable connecting Finland and Estonia being severely damaged, a telecom company operating in 60 countries facing a network disruption due to a cyber attack, and a hacktivist attack targeting an internet service provider (ISP) in Crimea.
- Significant **data exposure and leaks** incidents affected organisations in the air transport, law enforcement, banking and IT sectors.
- On the **hacktivism** front, in October, several groups of various origins claimed DDoS attacks in relation with the Israel-Hamas conflict.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in October 2023.

Europe

Cyber policy and law enforcement

EU announces possible stricter controls on critical technologies from spring 2024

Policy

On October 3, the European Commission adopted a recommendation on 10 critical technology areas for the EU's economic security for further risk assessment with Member States. Four technology areas will be assessed by the end of 2023: advanced semiconductors, artificial intelligence, quantum and biotechnology. The advanced connectivity, navigation and digital technology area, which includes cybersecurity technologies, is part of six other technologies areas that the Commission wants to start a conversation on with Member States.

European Commissioner issues letters to Meta and TikTok addressing the failure to curb disinformation

Regulation implementation

Between October 11 and 12, European Commissioner for the Internal Market, Thierry Breton, issued letters to the CEOs of the companies behind Meta and TikTok, stating that they have 24 hours from the date of the letter to address alleged illegal content and disinformation being disseminated about the Israel-Hamas conflict on their platforms. Failure of the social media companies to comply with the EU's Digital Services Act, could result in undisclosed penalty amounts. See also chapter "Information operations" below.

Ragnar Locker ransomware operation taken down after law enforcement operation

Takedown

Between October 16 and 20, an operation coordinated by Europol and Eurojust targeted the Ragnar Locker ransomware group. The operation followed an investigation led by the French National Gendarmerie, together with law enforcement authorities from Czechia, Germany, Italy, Japan, Latvia, the Netherlands, Spain, Sweden, Ukraine and the US. The "key target" of this malicious ransomware strain was arrested in Paris. The ransomware's infrastructure was seized in the Netherlands, Germany and Sweden and the associated data leak website on Tor was taken down in Sweden.

Spanish National Police arrest 207 suspected money mules linked to online banking scams

Arrest

The Spanish National Police have arrested 207 individuals suspected of being money mules involved in online banking scams across Spain. The scammers used tactics like spoofing bank telephone numbers to obtain victims' login credentials and conducted unauthorised money transfers, resulting in total losses of over 830.000 euros, as part of ongoing efforts to combat cyber fraudsters involved in various phishing scams.

Austrian Police dismantle illegal IPTV network, seize 1,6 million euros in assets

Arrest

The Austrian police have arrested 20 individuals involved in an illegal IPTV network that decrypted and redistributed copyright-protected broadcasts to thousands of customers between 2016 and 2023. The operation, which consisted of 80 perpetrators, primarily targeted Turkish citizens and operated through a hierarchy of suppliers and resellers, resulting in the seizure of 1,6 million euros from bank accounts, servers, luxury items, and numerous electronic devices.

Cyberespionage

Vietnam's Ministry of Public Security accused of using Predator spyware to target officials and journalists

Private sector offensive actor

An investigation by Amnesty International, conducted in collaboration with the European Investigative Collaborations (EIC), revealed Predator spyware attacks targeting civil society, journalists, politicians, and academics across the EU, the US, and Asia. The Predator spyware, developed by the Intellexa alliance, targeted UN officials, US Senator and Congressman, and Presidents of the European Parliament and Taiwan. These attacks used social media platforms like X (formerly Twitter) and Facebook to target 50 accounts belonging to 27 individuals and 23 institutions between February and June 2023. The investigation also uncovered evidence that a company within the Intellexa alliance signed a multi-million euro deal for "infection solutions" with Vietnam's Ministry of Public Security (MOPS) in early 2020.

Belarus-linked threat actor exploiting vulnerabilities in Roundcube webmail

Belarussian threat actor

According to ESET, the Winter Vivern threat actor exploited a zero day Cross-site scripting (XSS) vulnerability, tracked as CVE-2023-5631, in Roundcube webmail instances. The activity was detected on October 11. The group also exploited the issue CVE-2020-35730. Winter Vivern is a suspected Belarusian-origin APT group active since at least early 2021 and following pro-Russian objectives. In March 2023, it was reportedly engaging in a cyberespionage campaign targeting (and reported by) Poland and Ukraine.

Russian APT28 hackers breach critical networks in France, targeting government and institutions

Russian threat actor

On October 26, the French Agence National de Sécurité des Systèmes d'Information (ANSSI) published a report detailing tactics, techniques and procedures (TTPs) used the Russia-linked APT28 threat actor to target government entities, businesses, universities, research institutes, and think tanks in France since the second half of 2021.

Russia-linked threat actors exploit WinRAR vulnerabilities in Europe

Russian threat actor

On October 18, Google Threat Analysis Group (TAG) reported on multiple Russia-linked threat actors exploiting a known vulnerability, CVE-2023-38831, in WinRAR. WinRAR is a popular file archiver tool for Windows. One campaign impersonated a Ukrainian drone warfare training school. Another one attempted to deliver malware targeting energy infrastructure.

Malware campaign targeting Women Political Leaders summit, co-organised by European Parliament

Unattributed threat actor

According to a report Trend Micro on October 13, a threat actor dubbed Void Rabisu (a.k.a. Storm-0978) targeted EU military personnel and political leaders working on gender equality initiatives. The campaign, which was run between late June 2023 and August 2023, focused on attendees of the Women Political Leaders (WPL) Summit that was held in Brussels from June 7 to 8. Among the notable tools, Void Rabisu used Romcom RAT malware, of which it seems to be the exclusive user.

Cybercrime

Hackers continue targeting victims with Qakbot malware despite FBI takedown

Qakbot Malware

According to Cisco Talos researchers, despite the takedown of the Qakbot malware infrastructure (announced on August 30), hackers associated with Qakbot are still active and targeting new victims. They have been distributing various malware, including Ransom Knight ransomware, Remcos remote access trojan, RedLine information stealer, and Darkgate backdoor, with a campaign observed since early August, primarily targeting Italian-speaking users but also English and German-speaking individuals.

Banking malware targets Banking customers in Spain, Brazil, and Mexico

Banking trojan

According to ProofPoint, the banking malware Grandoreiro, operated by a threat actor tracked as TA2725, has expanded its targets to include bank customers in Spain, Brazil, and Mexico, using advanced phishing techniques that exploit a legitimate but vulnerable application. The malware gathers data via keyloggers or screen overlays, particularly targeting regions where cybersecurity awareness is low. This allows threat actors a large pool of potential victims.

Disruption

Finland-Estonia communications cable damaged

Telecommunications

An undersea communications cable connecting Finland and Estonia was severely damaged, alongside a gas pipeline, on October 8. Finnish authorities said the incident appeared to be a “deliberate, external act.” Finnish and Estonian authorities announced they were jointly investigating the situation, and the EU and NATO have offered support and condemned the attack. Despite the damage, Finnish officials have reassured that the country’s communication systems remained stable.

Lyca Mobile faces cyber attack and network disruption

Telecommunications

Lyca Mobile, a British telecom company operating in 60 countries, faced a network disruption due to a cyber attack over the weekend of September 30 - October 1. This affected service in most countries, causing difficulties in accessing their top-up portal and raising concerns about potential customer data compromise.

Pro-Ukraine hacktivist group IT Army takes responsibility for disruptive DDoS attacks on Crimea ISPs

Telecommunications

On October 27, the pro-Ukraine hacktivist group IT Army of Ukraine claimed responsibility for a DDoS attack targeting internet service providers in Crimea, which also reportedly affected the internet and telecommunications in Russia-occupied regions in Ukraine.

Hacktivism

NoName DDoS attacks against German targets

Germany

On October 2, NoName057(16), a pro-Russia supposed hacktivist actor, claimed DDoS attacks against German entities in the financial, transportation and government sectors. NoName referenced pro-Ukraine comments made by the German foreign minister in social media posts.

Pro-Russia hacktivists resume DDoS campaigns on EU targets after Israeli operations

EU

Pro-Russia hacktivists launched DDoS attacks against over 35 websites in several European countries, including Germany, France, Finland, Poland, Romania, Ukraine, and Albania, between October 11 and 12. These attacks, claimed by groups like Killnet and NoName, targeted public and private sector entities, and pro-Russia hacktivist groups are expected to continue such activities, with their focus shifting away from Israel and towards EU Member States.

South Asia based hacktivists target EU websites *EU*

On October 18, Mysterious Team Bangladesh, a pro-Palestine supposed hacktivist actor, claimed DDoS attacks against EU financial entities. On October 23, the same group also claimed DDoS attacks on Italian public service websites. On October 30, Team Insane Pakistan, another pro-Palestine supposed hacktivist actor, announced they would "start cyber attack on a number of countries," including EU countries who voted against a UN General Assembly Resolution over Gaza.

Information operations

Conversation AI fabricated circulated in Slovakia's elections *Deepfakes*

According to news sources on October 4, in the lead-up to Slovakia's elections, a fabricated conversation emerged featuring the leader of the party Progressive Slovakia and a local journalist. The conversation was later revealed to be a hoax created by an artificial intelligence tool.

TikTok sets up Command Center to Combat Israel-Hamas disinformation *TikTok*

On October 15, TikTok stated it immediately implemented appropriate resources and personnel to address concerns posed by the European Commissioner Thierry Breton, regarding alleged illegal content and disinformation being disseminated about the Israel-Hamas conflict on the platform. TikTok named the effort the Command Center to Combat Israel-Hamas Disinformation. See also chapter "Cyber policy and law enforcement" above.

Data exposure and leaks

Air Europa warns customers of data breach, urges credit card cancellation *Airlines*

Spanish airline Air Europa alerted its customers to cancel their credit cards following a data breach in which attackers accessed their card information. The exposed data includes card numbers, expiration dates, and CVV codes. The number of affected customers remains undisclosed at this time.

Unprotected database exposes Irish police and towing records *Police*

A security researcher discovered a non-password protected database with over 500.000 records related to the Irish National Police's car seizures and private towing and storage contractors. The exposed database contained various types of sensitive information, including identification documents, vehicle registration certificates, and insurance investigation inquiries. The researcher reportedly contacted the Irish National Police, and the database is now secure.

World

Cyber policy and law enforcement

Alliance of 40 countries to vow not to pay ransom to cybercriminals

Cooperation

The US White House announced that 40 countries in a US-led alliance plan to sign a pledge never to pay ransom to cybercriminals and to work toward eliminating the hackers' funding mechanism. The alliance aims to eliminate the criminals' funding through better information sharing about ransom payment accounts. Two information-sharing platforms will be created, one by Lithuania and another jointly by Israel and the UAE.

NSA to establish AI Security Center

Artificial intelligence

The US National Security Agency (NSA) has announced that it will be establishing an "AI Security Center" to consolidate its efforts in securing artificial intelligence (AI) systems. The center will aim to develop best practices and frameworks for AI security, focusing on protecting AI from vulnerabilities, digital attacks, and intellectual property theft, while collaborating with industry, academia, and international partners. The center will also oversee the development and integration of AI into US national systems.

SEC charges SolarWinds CISO with fraud for misleading investors before major cyber attack

Charge

The US Securities and Exchange Commission (SEC) plans to charge SolarWinds' Chief Information Security Officer (CISO), Timothy Brown, with fraud for misleading investors about cybersecurity practices. The complaint is related to SolarWinds' involvement in the December 2020's cyber attack attributed to the Russian Foreign Intelligence Service, involving malware insertion into their IT monitoring application.

US Supreme Court to judge on moderation of content

Social media

The US Supreme Court will review Texas and Florida laws that restrict social media platforms from moderating content, following challenges from tech industry groups claiming First Amendment violations. The case could set a precedent for the extent to which governments can regulate online speech.

Russia restricting VPNs

Internet control

According to a senator of Russia's ruling party, on October 3, Russia's communications regulator, Roskomnadzor, plans to block Virtual Private Networks (VPNs) starting March 1, 2024. The move comes after demand for VPNs surged following Russia's restrictions on Western social media platforms, including Meta Platforms' Facebook, Instagram, and WhatsApp, especially after Russia's military intervention in Ukraine in February 2022.

Malaysia alleges TikTok and Meta censoring pro-Palestinian content; Social media firms deny claims

Censoring

On October 26, Malaysia's Communications Minister Fahmi Fadzil accused social media platforms, including TikTok and Meta, of censoring pro-Palestinian content, warning of a "firm approach" if the issue wasn't addressed. Both TikTok and Meta denied the allegations, stating there was no truth to the accusations, emphasising their commitment to content moderation related to the Israel-Hamas conflict.

Israel freezes Hamas-linked cryptocurrency accounts amid conflict

Seizing

The Israel Police, in collaboration with various intelligence agencies and cryptocurrency exchange Binance, has frozen Hamas-linked cryptocurrency accounts used for fundraising during the Israel-Hamas conflict. While specific details regarding the number of accounts and the amount seized remain undisclosed, this move is part of Israel's ongoing efforts to seize cryptocurrency assets associated with militant groups and national security threats.

Cyberespionage

Gaza-linked cyber threat actor Storm-1133 targets Israeli energy and defence sectors

Palestinian threat actor

In its fourth annual Digital Defense Report, Microsoft revealed that a Gaza-based threat actor named Storm-1133 has been targeting Israeli private-sector energy, defence, and telecommunications organisations, with tactics involving social engineering and fake LinkedIn profiles to send phishing messages. Microsoft attributes the group's activities to furthering the interests of Hamas, with targets also including entities loyal to Fatah.

North Korean APT groups show increased coordination and complexity in cyber attacks

North Korean threat actors

In a report released on October 10, Mandiant assesses that North Korean state-sponsored APT groups have increased their coordination and collaboration, making it harder for investigators to attribute cyber attacks to specific groups. The APTs have diversified their attacks and are sharing tools and code, posing a challenge for defenders to track and attribute malicious activities accurately.

North Korean groups conduct supply chain attack through TeamCity

North Korean threat actors

On October 18, Microsoft reported that it observed Diamond Sleet and Onyx Sleet, two North Korean nation-state threat actors, exploit CVE-2023-42793 since early October. CVE-2023-42793 is a remote-code execution vulnerability affecting multiple versions of JetBrains TeamCity server.

Grayling: new APT group targets organisations for intelligence gathering

Unattributed threat actor

According to Symantec, a new APT group, tracked as Grayling, has been discovered targeting organisations in Taiwan, Pacific Islands, Vietnam and the US. Using a mix of custom malware and publicly available tools, Grayling's motive appears to be intelligence gathering, with a focus on sectors such as manufacturing, IT, biomedical, and government, indicating a preference for data collection over financial gain.

Powerful StripedFly malware disguised as crypto miner infects 1 million Windows and Linux PCs, evading detection for over 5 years

Unattributed threat actor

Kaspersky has uncovered a sophisticated malware called StripedFly that masquerades as a cryptocurrency miner to evade detection and has infected over 1 million Windows and Linux computers worldwide since 2016. The malware, which incorporates an NSA-developed exploit called EternalBlue, infiltrates unpatched Windows systems, spreads across networks, and can harvest sensitive data, capture screenshots, gain control over machines, and record microphone input, all while maintaining a cryptocurrency mining module to divert attention from its true capabilities.

Cybercrime

Hunters International ransomware emerges, potentially linked to Hive gang resumption

Ransomware

A new ransomware-as-a-service called Hunters International has emerged, using code from the Hive ransomware operation, suggesting that the Hive gang may have resumed activity under a different name. Security researchers have identified strong code overlaps between the two ransomware groups, although Hunters International claims they purchased the source code from Hive developers and focus on data theft rather than encryption.

Magecart campaign utilises innovative technique to hide credit card skimming code

Magecart

Magecart, a consortium of malicious cybercriminals who target online shopping cart systems, have employed a novel technique, hiding JavaScript code within a comment on a targeted site's 404 default page, allowing them to steal credit card information from visitors to major websites undetected for weeks. This technique represents a significant evolution for Magecart, as it enables them to hide their code amid the complexity of modern websites, making detection more challenging.

Israel's national cyber directorate warns of WhatsApp scammers exploiting Israel-Hamas conflict

WhatsApp Scam

The Israel National Cyber Directorate (INCD) has issued a warning about scammers sending unsolicited WhatsApp messages to Israelis amid the Israel-Hamas conflict. The scammers claim to possess critical information about individuals held hostage in the Gaza Strip, requesting a "proof fee" of approximately 255 US dollars, prompting the INCD to advise users to enhance online security measures and avoid sharing sensitive information in large groups on social media while advocating for multi-factor authentication and unique passwords.

Data exposure and leaks

Third Flagstar bank data breach affects 800.000 customers due to MOVEit exploit in Fiserv breach

Banking

Flagstar Bank has reported its third data breach since 2021, affecting over 800.000 US customers. This breach was a result of a cyber attack on a third-party service provider, Fiserv, where attackers exploited a zero day vulnerability in the MOVEit Transfer product to access Fiserv's systems, subsequently stealing Flagstar customer data.

D-Link employee falls for phishing leading to data breach

IT

D-Link Corporation, a Taiwanese networking equipment, disclosed that on October 2 it received a claim of a data breach from an online forum by an unauthorised third party. The intrusion vector was likely an employee who unintentionally fell victim to phishing.

Disruption

Israeli civilian aircraft affected by GPS jamming prior to Hamas attack

Israel

In late September 2023, passenger planes approaching Ben-Gurion International Airport had to alter their flight paths due to "severe" GPS navigation issues, which Israeli authorities deemed an "attack" on Israel. The GPS jamming had been ongoing for months, with potential sources including Russia's electronic warfare units in Syria, unknown sources in Syria and Lebanon, or Iran, although no concrete evidence linked the incidents to the recent Hamas attack on Israel.

BiBi-Linux: A new wiper dropped by pro-Hamas hacktivist group

Israel

According to the Israel-based Security Joes incident response company, a hacktivist group affiliated with Hamas conducted a cyber attack on Israeli companies. The cyber weapon used in the attack, called "BiBi-Linux," was designed to destroy infrastructure and included references to the Israeli Prime Minister's name, with no ransom note or command-and-control servers, indicating its intent for data destruction.

Hacktivism

Pro-Russia groups target Israeli organisations amid conflict

Israel - Hamas

Following the deadly attack by Hamas on October 7, pro-Russia groups like Killnet and Anonymous Sudan started targeting Israeli government and media websites, claiming “”Israeli government, you are responsible for this bloodshed.”

Pro-Hamas groups target power grid and infrastructure in Israel amid conflict

Israel - Hamas

Pro-Hamas groups like Cyber Av3ngers targeted power grid organisations, including the Israel Independent System Operator, and claimed to have compromised their networks and disrupted their websites. Pro-Palestine hacker groups like Ghosts of Palestine and several others called on hackers worldwide to attack infrastructure or organisations in Israel or in countries perceived as supporting Israel.

Israel-linked hacking group, Predatory Sparrow, resurfaces amid conflict

Israel - Hamas

After a year of silence, the hacking group Predatory Sparrow, suspected of having ties to the Israeli government, has reemerged online. As the Israel-Hamas conflict continues, various hacktivist groups on both sides have engaged in DDoS attacks and defacements of websites, signalling an increased digital presence in the conflict. Among these groups, Predatory Sparrow stands out due to its history of sophisticated attacks, particularly against Iran, and its strategic approach, which focuses on signalling capabilities through restraint.

South Asian hacktivist groups align ideologically in Israel-Hamas war response

Israel - Hamas

After October 7, South Asian hacktivist groups responded to the Israel-Hamas war based on their ideological alignments. Pro-India groups targeted Palestinian entities. Hacktivists from Muslim-majority South Asian countries, including Mysterious Team Bangladesh and Team Insane PK targeted Israeli entities or countries perceived as supporting Israel. Indian Cyber Force (ICF) allegedly disrupted access to Palestinian entities, including a Hamas website, a telecommunication company, a bank, a government e-mail service, a transportation entity, and an ecommerce website, with the prominent groups Indian Cyber Force.

Information operations

Russian propaganda spreads fake news about Ukrainian weapons in Hamas amid Israel conflict

Israel - Hamas

Russian propaganda has been spreading fake reports suggesting that Hamas terrorists are using weapons from Ukraine amid the ongoing conflict between Hamas and Israel, according to Ukraine’s Center for Countering Disinformation. Russian Telegram channels have launched an information campaign to discredit Ukraine and its military forces, falsely claiming that Ukraine is supplying weapons to Hamas, while also reporting that Israeli forces captured Hamas terrorists with Ukrainian weapons.

AI-powered impersonation of Sudanese ex-leader Omar al-Bashir spreads confusion on TikTok amid civil war

Sudan Crisis

An anonymous campaign using artificial intelligence to impersonate former Sudanese leader Omar al-Bashir has gained hundreds of thousands of views on TikTok, causing confusion amid the country’s ongoing civil war. The AI-generated “leaked recordings” of Bashir have been posted on a TikTok channel called The Voice of Sudan, highlighting concerns about the rapid dissemination of fake content through social media and the potential for disinformation to disrupt fragile situations like Sudan’s crisis.

Significant vulnerabilities

GNU C Library Dynamic Loader Buffer Overflow Vulnerability
A critical buffer overflow vulnerability, identified as CVE-2023-4911, has been discovered by Qualys Research Labs in the GNU C Library's dynamic loader when processing the "GLIBC_TUNABLES" environment variable. This vulnerability can be exploited to obtain full root privileges, impacting several major Linux distributions See CERT-EU's SA 2023-072.

GNU C Library

Access Control Vulnerability in Confluence Data Center and Server
Atlassian has been made aware of a critical vulnerability, CVE-2023-22515, a Broken Access Control vulnerability in Confluence Data Center and Server. External attackers may exploit this vulnerability in publicly accessible Confluence Data Center and Server instances to create unauthorised Confluence administrator accounts and access Confluence instances. Atlassian Cloud sites are not affected by this vulnerability. See CERT-EU's SA 2023-073.

Atlassian Confluence

HTTP/2 Rapid Reset DDoS Vulnerability
On October 10, Cloudflare, Google and Amazon AWS, jointly disclosed a vulnerability affecting the HTTP/2 protocol. Named as CVE-2023-44487, this vulnerability impacts various web services and cloud customers. This vulnerability is being actively exploited and has led to Distributed Denial of Service (DDoS) attacks that are significantly larger than previous Layer 7 attacks. See CERT-EU's SA 2023-074.

HTTP/2

Citrix NetScaler Critical Vulnerability
On October 10, Citrix issued an advisory about multiple buffer-related vulnerabilities, CVE-2023-4966 and CVE-2023-4967, affecting NetScaler ADC and NetScaler Gateway. These vulnerabilities can result in sensitive information disclosure and denial of service attacks. See CERT-EU's SA 2023-075.

Citrix NetScaler

Vulnerability in cURL and libcurl
A security vulnerability in the cURL tool and libcurl library has been identified. This flaw enables a heap-based buffer overflow during the SOCKS5 proxy handshake, potentially allowing malicious actors to execute arbitrary code (RCE). At this time, CERT-EU is not aware of any active exploits leveraging this vulnerability. The vulnerability affects libcurl versions 7.69.0 to 8.3.0. The issue was reported on September 30, 2023, and a patch has been released in curl version 8.4.0. The vulnerability is tracked as CVE-2023-38545. See CERT-EU's SA 2023-076.

cURL

Microsoft October 2023 Patch Tuesday
Microsoft has released its October 2023 Patch Tuesday Security Updates, addressing a total of 103 CVEs among which 12 are rated as critical, and 91 are rated as important. Microsoft also reported that two vulnerabilities are actively exploited. See CERT-EU's SA 2023-077.

Microsoft _

Cisco IOS XE Software Web UI Privilege Escalation Vulnerability
On October 16, Cisco published an advisory regarding a critical vulnerability, CVE-2023-20198, affecting the Web UI of Cisco IOS XE Software. This vulnerability could allow an unauthenticated remote attacker to create a privileged level 15 account, granting them control over the affected system. The vulnerability has a CVSS score of 10. See CERT-EU's SA 2023-078.

Cisco IOS XE

Juniper Networks Junos OS Multiple Vulnerabilities
On October 14, Juniper Networks announced patches for more than 30 vulnerabilities in Junos OS and Junos OS Evolved, including nine high-severity flaws. The most severe vulnerability, tracked as CVE-2023-44194 with a CVSS score of 8.4 out of 10, allows an unauthenticated attacker with local access to create a backdoor with root privileges due to incorrect default permissions in a certain system directory. See CERT-EU's SA 2023-079.

Juniper Networks Junos OS

Multiple Vulnerabilities in SolarWinds Access Rights Manager (ARM)

SolarWinds Access Rights Manager

On October 18, SolarWinds announced patches for eight vulnerabilities in Access Rights Manager (ARM) including eight high-severity flaws. The most severe vulnerabilities are tracked as CVE-2023-35182 and CVE-2023-35184 for Remote Code Execution Vulnerability, as well as CVE-2023-35185 and CVE-2023-35187 for Directory Traversal Remote Code Vulnerability, with a CVSS score of 8.8 out of 10. See CERT-EU's SA 2023-080.

Multiple Vulnerabilities in VMware Aria Operations for Logs

VMware Aria Operations

On October 19, VMware has released security updates to address two vulnerabilities affecting Aria Operations for Logs. The exploitation of the vulnerabilities could lead to Remote Code Execution and Authentication bypass. The vulnerabilities are tracked as CVE-2023-34051 and CVE-2023-34052 with a CVSS score of 8.1. See CERT-EU's SA 2023-081.

Multiple Vulnerabilities in LifeRay products

LifeRay

This security advisory addresses multiple vulnerabilities in Liferay Portal and Liferay DXP related to cross-site scripting (XSS) attacks. See CERT-EU's SA 2023-082.

Critical Vulnerability in F5 BIG-IP Configuration utility

F5 BIG-IP

On October 26, F5 released a security advisory for a critical vulnerability impacting BIG-IP that allows a user to perform remote code execution. The vulnerability is tracked as CVE-2023-46747 with a CVSS score of 9.8 out of 10. See CERT-EU's SA 2023-083.

Critical Vulnerability in VMware products

VMware

On October 25, VMware has released security updates to address two vulnerabilities affecting vCenter Server and Cloud Foundation. The exploitation of the vulnerabilities could lead to an out-of-bounds write and a partial information disclosure. The vulnerabilities are tracked as CVE-2023-34048 with a CVSS score 9.8 and CVE-2023-34056 with a CVSS score of 4.3. See CERT-EU's SA 2023-084.

Critical Vulnerability in Confluence Data Center and Server

Confluence

On October 30 2023, a notable vulnerability, CVE-2023-22518, affecting Confluence Data Center and Server was disclosed by Atlassian. The exploitation of this vulnerability could result in significant data loss. Updates are already available for this vulnerability. The CVE-2023-22518 has a CVSS score of 9.1 indicating a critical risk. See CERT-EU's SA 2023-085.

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.

TLP	Disclosure	Message
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.