Threat Highlight Report

May 2024

WITH secure

Contents

Foreword

This month has seen both positive and less positive cybersecurity news. The law enforcement action against LockBit continues with the naming of the person believed to operate LockBit and the LockBitSupp persona, though it seems LockBit responded to that by posting a large number of victims to its leak site this month.

The US government cybersecurity agency, CISA has initiated a secure by design pledge, which many significant software solution providers have signed up to, but at the same time yet another major player in the SSL VPN market, CheckPoint, have experienced a zero-day vulnerability in their CheckPoint Firewall VPN gateways. Recognizing the repeated zero-days in SSL VPN/Web VPN solutions, Norway's NCSC have recommended that organizations stop using them and move to either IPSec IKEv2 VPNs, or even just 5G data connections.

This was also the month for statistics and summaries regarding 2023, with no less than 5 different companies publishing their round up and analysis.

For the first time we also include a section purely on AI security news, as 5 pieces of news about AI met the threshold for inclusion this month.

- Stephen Robinson, Senior Threat Intelligence Analyst, WithSecure

1 Monthly highlights

1.1 Checkpoint VPN gateways under zero-day attack

Checkpoint Firewall VPN gateways are under attack from a threat actor who is specifically targeting Checkpoint VPN local accounts. These are accounts which are configured on the VPN device itself, instead of being Active Directory or LDAP accounts. The reason they are being targeted is because they only use password-based authentication, and because the authentication is local to the VPN device. As such there is no MFA, and there may not be any central logging or account lockouts in response to brute force, password guessing attacks. This is recorded as CVE-2024-21914 and applies to Checkpoint Security Gateways with the Remote Access VPN or Mobile Access blades enabled. Checkpoint have provided a hotfix which disables/removes all such VPN local accounts, but currently at the end of May there were estimated to be 13,000 Checkpoint VPN gateways exposed to the Internet. It is unknown how many of those have received the hotfix, but it gives an idea of the scale of this problem. With this issue, Checkpoint joins the long list of VPN gateway solution providers who have suffered zero-day vulnerabilities in their products this year.

WithSecure Insight

Infrastructure appliances, such as CheckPoint Firewalls, are often embodiments of the phrase “if it isn’t broke, don’t fix it”. As such they can often be old operating systems or software layered with new additions. In this case it seems that an older piece of functionality, VPN/device local accounts, is vulnerable precisely because it was not changed to keep up with the changing threat landscape. At this time any public-facing authentication process which does not use MFA is vulnerable, and attackers are specifically hunting for these MFA-less processes in order to exploit them. After the success of this campaign, if any other VPN gateway solutions have similar functionality we can be confident that we will see attackers targeting those other solutions, also.

1.2 Secure by Design pledge

At RSA Conference this year CISA announced that 68 leading software manufacturers have signed a voluntary pledge to begin implementing a secure by design ethos, building in security from the beginning of their product lifecycle. The pledge explicitly states that companies will:

- Increase the use of MFA
- Reduce the use of default passwords
- Reduce the prevalence of certain types of vulnerabilities
- Attempt to improve patching rates
- Publish a vulnerability disclosure policy
- Improve CVE disclosure transparency
- Increase customers' ability to gather evidence of cybersecurity intrusions affecting their products

WithSecure Insight

Among the signatories of the pledge are Microsoft, Cisco, Fortinet, GitHub and GitLab, Ivanti, Okta, and Palo Alto. All of these are organizations which have either experienced significant breaches, and/or been the cause of significant breaches of their customers through vulnerabilities in their software and services. As has been covered in previous THRs, several of these organizations have patched large numbers of vulnerabilities in their products in recent months, something which may have been motivated by this pledge. Alternatively, their actions may have been motivated by the same thing that has caused CISA to create the Secure by Design pledge - the many significant incidents and campaigns caused by supply chain breaches and campaigns of mass exploitation. Whatever the cause, and whatever questions this may raise regarding their design ethos before this pledge, this is definitely a step, and hopefully multiple steps in the right direction.

1.3 SSL VPNs – Just say no

The Norwegian National Cyber Security Centre have made an official recommendation that organizations should stop using SSL VPN or Web VPN solutions and replace them with IPSec IKEv2 based solutions, with a target adoption date for CNI entities of the end of 2024, and end of 2025 for other organizations.

SSL VPN vulnerabilities in market leading VPN gateway products have been the cause of a number of major breaches and campaigns in recent years, as reported in previous THRs, and Norway are not the only country to recommend dropping them in favor of IPSec IKEv2 VPNs, both the United States and the United Kingdom also recommend this.

One good reason why switching to IPSec could improve security is that IPSec (and IKEv2) is a defined open standard which is currently considered to be secure. SSLVPNs and Web VPNs are not open standards, they are more like proprietary products, where each vendor has attempted to create their own secure solution, with varying success. The N-NCSC recommends reconfiguring or replacing existing VPN solutions, disabling SSL VPN functionality, and if IPSec is not possible, using 5G Broadband. For organizations who are not currently able to migrate to IPSec IKEv2 VPNs, they recommend:

- implementing centralized VPN logging
- implementing strict geofencing restrictions
- blocking access from VPN providers, VPS providers, and Tor exit nodes

WithSecure Insight

It is true that there have been a distressing number of vulnerabilities in SSL/Web VPN gateways in recent months and years, with multiple mass exploitation events targeting those vulnerabilities. This has affected so many major solution vendors in this space that at this point simply avoiding all solutions of this type does seem like quite a reasonable suggestion. IPSec VPN solutions are obviously not necessarily absolutely secure, but because they are based on a publicly published, peer reviewed IETF specification there is less scope for variation and vulnerabilities in any implementation that follows the specification correctly. In addition to this, it should be relatively simple for any organization with an SSLVPN to move to an IPSec VPN without too much disruption. It is also worth noting that all of the additional recommended mitigations for those unable to migrate to IPSec VPNs are equally as useful for IPSec VPNs, or any other type of remote access.

1.4 Ransomware, espionage, and statistics

It appears that this is the month for 2023 trend reports, with research from Verizon, Rapid7, Huntress. Sophos, and BitSight.

BitSight do Internet scanning to identify devices that are vulnerable to exploitation. While they cannot identify all CVEs through their scanning, they can identify what they believe to be a representative subset. Through this they have observed that vulnerabilities which are added to CISA's KEV have a median remediation time of 174 days, while non-KEV CVEs are remediated in 621 days. 35% of the organizations BitSight have visibility of had at least one publicly exposed KEV CVE in 2023.

Verizon meanwhile gave statistics relating to the 30,458 data breaches they investigated in 2023 and observed that organizations took an average of 55 days to remediate 50% of KEV vulnerabilities, which suggests a more rapid response time than that given by BitSight. However, they also state that the median time until a KEV CVE is targeted for mass exploitation is 5 days. Giving some incident statistics, Verizon stated that 14% of breaches in 2023 had an initial attack vector of vulnerability exploitation, a 180% Year on Year increase. 15% of breaches were supply chain attacks, a 68% YoY increase, and that 32% of breaches involved extortion. Verizon have noted however that a rather significant 8% of all data breach incidents they dealt with in 2023 were caused by MOVEit, which on its own accounts for a significant part of the bump in both vulnerability exploitation, supply chain, and extortion incidents. Interestingly, this also tells us that Verizon alone investigated 2,400 MOVEit incidents, though because these incidents often had multiple victims per compromise, it may be possible Verizon were engaged multiple times for a single compromise.

Rapid7 found that in the attacks they investigated, 53% of mass compromise events arose from zero-days compared to n-days, and that more than 60% of vulnerabilities in infrastructure devices were exploited as zero-days. They also observed that exploitation of network edge devices almost doubled in their data since the beginning of 2023, with 36% of widely exploited vulnerabilities occurring in network perimeter devices. They also stated that 23% of zero-day mass exploitation events were a single actor compromising tens or hundreds of organizations at once with their own custom tooling, something they attribute to the existence of a mature, well-organized cybercrime ecosystem. Moving away from vulnerabilities, they stated that 47% of incidents were the result of missing or unenforced MFA on internet facing systems. Rapid7 also stated that they believe there was a distinct drop in the number of unique, new brands operating in 2023, as actors coalesced around fewer, major brands.

In Huntress' trend analysis of 2023 however, they stated that there was an increasingly diverse ransomware landscape, with more affiliates and entities operating outside of the major brands. Huntress associate this with the Qakbot takedown in August 2023, observing that there was a surge in both ransomware activity and the number of different active threat actors, with an increase in ransomware attacks that specifically target small businesses and MSPs.

Sophos published the results of a survey of a large number of cybersecurity leaders which found that 99% of organizations affected by ransomware identified the root cause of the attack, and that in 32% of cases in 2023 it was vulnerability exploitation, followed by compromised credentials at 29%. 94% of respondents who suffered attacks said that ransomware attackers attempted to compromise backups as part of the attack, and 57% of those attempts were successful. When backups were compromised things then got much worse for the victims, with ransom demands typically more than doubling, median recovery costs increasing from $375,000 to $3million, and the likelihood of paying the ransom increasing from 36% to 67%. Once again illustrating the variability of statistics, Sophos observed that 46% of victims among their respondents paid ransoms in 2023, the same proportion as in 2022, but an almost 50% increase on 2021.

WithSecure Insight

Statistics give us a way to draw insights and (hopefully) understanding from this complex landscape. As ever, statistics do not give us the whole story, they give us information about the data set they were drawn from. Verizon and BitSight seem to disagree on the time taken to patch KEV vulnerabilities, however Verizon's data appears to apply to any KEV vulnerability while BitSight's applies to a subset of Internet facing, detectable vulnerabilities. Huntress and Rapid7 appear to be disagreeing, as Rapid7 says there are fewer ransomware brands, while Huntress says there are more distinct threat actors. What every report does seem to agree on however is that mass exploitation as an initial access vector has grown, though Verizon and Rapid7 both observe that a some of that increase at least is due to the actions of a small number of highly proficient actors. What is very important to note for anybody who is considering making decisions based on these statistics, is that these are generalizations. The types of attacks, infection vectors, and the results of those attacks actually differ by geography, sector, and average revenue. Security threats and goals for the midmarket are likely to differ compared to large enterprises.

2 Ransomware: Trends and notable reports

2.1 The numbers

Numbers have sharply risen from April (402) to May, where 528 new victims have been added to ransomware leak sites. 528 represents the busiest single month on breach sites since September 2023. This is largely due to a large number of victims posted by LockBit 3.0, demonstrating just how influential LockBit is over the ransomware market.

Ransomware	Count	Change
3AM	2	1
8BASE	21	-4
Abyss	1	0
Akira	20	2
Apos Security	0	-4
Arcus Media	11	11
BianLian	14	3
BlackBasta	17	-7
Blackout	1	0
Blacksuit	15	-6
Cactus	7	-6
CiphBit	0	-4
CL0P	3	0
Cloak	3	-5
Daixin	0	-1
dAnon	4	-4
DarkVault	3	-14
Data Leak	1	-8
Defray777	0	-1
Dispossessor	1	0
Donut Leaks	2	2
DragonForce	13	1
Dunghill Leak (News)	0	-1
Embargo	3	1
Eraleignews	4	2
Everest	5	3
FSOCIETY	5	5
Hunters International	11	-18
INC Ransom	33	18
Kill Security	2	1
LockBit	174	149
MalekTeam	0	-2
Mallox	1	0
Medusa	24	-4
Meow	1	1
MetaEncryptor	4	4
Money Message	1	1
Monti	4	4
MyData	0	-2
Play	32	2
Qilin	19	7
Qiulong	1	-5
RA Group	5	-9
Ransomhouse	11	5
RansomHub	27	4
Red Ransomware	3	2
Rhysida	6	0
Snatch	1	1
Space Bears	2	-6
Stormous	6	5
Underground	3	1
Zero Tolerance	1	1

2.1.1 Monitoring LockBit

LockBit numbers are extremely high this month. This comes after the actor LockBitSupp was named by law enforcement (more on this later). Two days after his outing, LockBit's leak site started posting a large number of victims in what was almost certainly a reactionary move. In total, 257 victims were posted to LockBit's breach site, of which 83 were duplicates of older ransomware events. Regardless of these, LockBit posted 174 previously unseen victims, and despite analysis on these suggesting that many of the file archives/dumps are some months old based on their most recently modified file, this is the second busiest month for a single RaaS leak site since monitoring started in 2022 (the busiest being Clop following the MOVEit mass-compromise events).

2.1.2 New groups

A relatively small number of newcomers entered the scene this month with only three new leak sites observed. These were Arcus Media, FSOCIETY and Zero Tolerance:

- FSOCIETY posted five victims, and while it is probably a reference to the hacker society in the TV drama Mr Robot, they were also noted as a partner in RansomHouse's Partners page on their DLS, making it inherently possible they are more experienced actors attempting to manage their own extortion operations.
- Arcus media posted 11 victims in May, which is relatively high for a 'newcomer'. Its origins are unknown, however there is a definite skew towards South America in its victimology.
- Zero Tolerance only posted one victim in May 2024

2.2 Ransomware extortion methods

Mandiant have observed increasingly personal aggressive tactics being employed by ransomware groups as part of their negotiating tactics during extortion operations. This included SIM swapping the children of executives in order to make phone calls coming from the phone numbers of their children. This and other coercive tactics have been employed by attackers, such as directly contacting executives and their family members at home, essentially applying personal pressure to the decision makers at victim organizations.

2.3 LockBit leader named by law enforcement

US, UK, and Australian law enforcement have charged and sanctioned one Dmitry Yuryevich Khoroshev as the alleged leader of the LockBit ransomware group. While LEA have not said how they identified him, investigative journalist Brian Krebs of KrebsOnSecurity detailed the identities and communications associated with Dmitry from 2010-2016, after which he vanished from view. These indicate that the named individual was an active coder selling malicious code and services in Russian cybercrime forums during the formative years of ransomware, but that those early personas went dark several years before the LockBit operation began. It is almost certain that LEA have more information than they are not sharing, but unless this case ends up going to court somehow, it is unlikely that we will find out what that information is.

2.4 BlackBasta use Microsoft QuickAssist in social engineering attacks

Microsoft have stated that the BlackBasta ransomware group has been seen using voice calls (vishing) as an initial access vector, social engineering victims into allowing the attacker access via the inbuilt Microsoft RMM, QuickAssist. Microsoft have suggested that organizations can protect themselves against abuse of QuickAssist by blocking or uninstalling QuickAssist in their environment if it is not in use, although they also observe that multiple other RMMs have been used in similar attacks, including ScreenConnect and NetSupport Manager.

2.5 BlackBasta claims hack of Atlas Oil

BlackBasta have also claimed to have hacked Atlas Oil, one of the major oil distributors in the US who supply 1 billion gallons of oil per year. The attackers claim to have stolen 730GB of data and have leaked documents as proof of the hack, however as of yet there has been no comment from Atlas.

3 Hacktivism

3.1 Sweden targeted by DDoS attacks upon joining NATO

According to information from NetScout, Since the beginning of 2023 Sweden has seen an increase in DDoS attacks from Russian aligned hacktivist groups associated with their joining of NATO. The volume of attacks increased distinctly in February, and 3 days after Hungary indicated that they would most likely approve Sweden's application to join NATO there were 1,500 DDoS attacks against Swedish organizations. In comparison, in January there were very rarely ever more than 1,000 attacks per day.

In March, 3 days before Sweden joined NATO, NetScout observed 2,200 attacks, a 183% increase on the same day in 2023. Numbers of DDoS attacks have continued to increase ever since, rising to a new average somewhere between 1,000 and 1,500 attacks per day. NetScout saw attacks from multiple Russian-aligned hacktivist groups, including NoName057, Anonymous Sudan, Russian Cyber Army, Killnet. These are groups who in some cases appear to overlap or reference each other, and NoName057 was linked to the Russian state threat actor Sandworm by recent Mandiant reporting.

3.2 Links between Iranian APTs and hacktivist groups targeting Israel

Checkpoint have published an article regarding Void Manticore, a group who perform destructive wiper attacks and influence operations who have been linked to Iran's Ministry of Intelligence and Security. They observed Void Manticore operating hacktivist personas "Homeland Justice" targeting Albania, and "Karma" targeting Israel, and also observed indications of another Iranian APT, Scarred Manticore, handing off their victims to Void Manticore for destructive attacks to be carried out. Scarred Manticore appear to perform stealthy, long-term access compromises against their victims, harvesting emails and deploying stealthy payloads, whereas Void Manticore tends towards rapid, noisy attacks culminating in deployment of the Bibi wiper malware.

WithSecure Hacktivism Insight

Cyber-attack targeting is heavily influenced by real world events. The invasion of Ukraine has given repeated examples of this, with destructive cyber-attacks against critical infrastructure, stealthy intelligence gathering operations, and misinformation and influence campaigns a hallmark of the conflict. The increased targeting of Sweden during the process of joining NATO illustrates how Russia uses these DDoS hacktivist groups to express their displeasure. These groups have long been thought to be merely intelligence agency sock-puppets, but it seems unlikely that their DDoS attacks will actually change the course of a nation. A more likely explanation is that they are low effort ways to generate headlines which will increase reporting and coverage of the Russian propaganda messaging that these groups regularly parrot alongside their attack declarations.

There is of course the possibility that these noisy attacks are simply a form of digital chaff to hide something stealthier. That may well have been the case with the Iranian APT/hacktivist overlap. In most large organizations with regular backups and cloud storage, wipers are not going to have much of an effect, but one thing they will do is make it much harder to recover forensic information about an attacker's actions on the network, and even if any indications of compromise do persist, it is likely that they will be attributed to the very obvious, loud, low skill wiper attack, instead of being taken as evidence of a stealthy APT operation preceding that.

4 Other notable highlights in brief

4.1 Change Healthcare compromised via MFAless Citrix account

Change Healthcare have provided an update to their investigation into how they were compromised by associates of the ALPHV ransomware gang. In testimony by the CEO before a US government committee it was stated that the attackers used stolen credentials to login to their Citrix remote access service, which was not protected with multi factor authentication. The attackers gained access on the 12th of February, and the ransomware detonation occurred on the 21st.

WithSecure Insight

It is absolutely vital to use MFA, as it can truly make the difference between being compromised or being secure. In this case this was a $1.6 billion dollar oversight. In this day and age any authentication system should have MFA enabled, and if for some reason a legacy system must be used where it is not possible to implement MFA it should not be publicly accessible.

4.2 Microsoft announce organizational change to address security failures

While we believed it would take time for Microsoft to enact change in response to the recent CSRB investigation, it has already announced a series of organizational changes. The pay awards of some senior executives will be tied to prioritizing security over shipping new features, deputy CISOs will be partnered with engineering teams, and executives will meet weekly to assess the execution of these new security priorities.

WithSecure Insight

These announcements from Microsoft indicate the beginning of movement in the correct direction, however corporate change takes time, as well consistent, concerted effort. In 12 months, we may well see what the result of this new organizational priority was or will be.

4.3 MITRE ICS hack began in December 2023, employed rogue VMs

MITRE have continued to be open about the events surrounding their compromise by a Chinese state sponsored actor who exploited a zero-day vulnerability in an Ivanti ConnectSecure appliance to access their network. They identified that they were in fact compromised in December 2023, so well before any of the Ivanti related malicious activity came to light. After gaining access to the network the attackers obtained an administrative password to a VMWare vCenter management server. They installed webshells on the vCenter server, but they also created VMs directly on ESXi servers, bypassing vCenter to create what are termed “Rogue VMs”. Because these VMs were not created through vCenter, then vCenter is completely unaware of them. As such, defenders were unaware of them, and the attackers were able to use them to access the webshells they had deployed on the vCenter management server.

The only way to detect Rogue VMs is by using the command line of the ESXi appliance to list existent VMs, then compare that list to the VMs that vCenter is aware of. MITRE have published scripts that can be used to identify rogue VMs in this way, which can be incorporated into security monitoring for ESXi environments.

WithSecure Insight

Once again, it is excellent to see such clear communication from MITRE. They have provided not only valuable information on the operations of this advanced persistent threat, but also details of a common blind spot in the defenses of many organizations, along with tools to address that blind spot. It is excellent to see hard earned security advantages being shared like this.

4.4 Cuttlefish router malware parses traffic for sensitive data

Researchers at Lumen technologies have reported on a piece of SOHO router malware they have named Cuttlefish, which due to code overlaps they believe is related to HiatusRAT. Cuttlefish is a modular malware which infects Small Office/ Home Office (SOHO) routers, and while it has only been observed infecting devices on a particular Turkish ISP, it has some interesting functionality. Among other modules and functions, Cuttlefish is able to parse the traffic traversing the router to look for authentication traffic to certain sites, and it can then record or proxy that traffic to another destination, which could allow attackers to perform attacker in the middle (AITM) masquerade attacks, or similar. While Lumen have not attributed the campaign, they have observed that HiatusRAT was previous used by Chinese nexus attackers.

WithSecure Insight

While this malware appears to have been limited to a single Turkish ISP, that focused distribution combined with the ability to steal authentication information for specific services from traversing traffic is very interesting. This functionality could be extremely useful to espionage and financially motivated attackers, enabling a mass exploitation campaign to stealthily intercept and acquire valuable credentials for cloud services which could be used for further access.

4.5 Even larger US healthcare provider takes systems offline after “cybersecurity event”

Ascension Healthcare is a US healthcare provider that operates 140 hospitals and 40 care homes across 19 states. They have an annual turnover of $28 billion (6 times that of Change Healthcare) and they have recently taken systems offline in response to a cybersecurity event. Whatever that event was it was detected on the 8th of May, they advised their business partners to sever all connections to their network and services until further notice, and as of their last update on the 24th of May they were still working to restore operations. While hospitals and facilities remain open and functional, there is the distinct possibility that this could be yet another major data theft/extortion case affecting the US healthcare sector.

WithSecure Insight

Considering the impact of the Change Healthcare ransomware incident, it is entirely plausible to conclude a ransomware attack on an even larger US healthcare organization could have a similarly larger impact. However, Change Healthcare offered payment services, so while its revenue may have been lower, it most likely had an impact on a very large number of customers and suppliers when its systems went down. Ascension directly operates hospitals and care homes, so an outage of its systems is likely to be more localized, with fewer knock-on effects on others. Unfortunately, because this is a direct healthcare provider, those localized effects could well have a life-or-death impact on individuals at Ascension hospitals. That of course is most likely part of the reason why the healthcare sector has seen such a surge of ransomware attacks in recent years however, because in that sector, recovery from a cyber incident truly is a life-or-death situation.

4.6 ICS modems vulnerable to RCE via SMS

Telit Cinterion cellular modems are widely used in sectors including industrial, healthcare, and telecommunications. A total of 8 CVEs have been disclosed by researchers from Kaspersky’s ICS division, the most concerning of which is CVE-2023-4761, which allows for remote code execution via SMS, and has been assigned a severity score of 9.8. Remediation of this vulnerability will most likely be complicated by the fact that these modems may well be used in devices which are not easily accessible, and because the affected devices are modems, they are by definition public facing.

WithSecure Insight

A vulnerability in a modem is extremely concerning, as by definition these devices sit on the very outside of any network. They are low level devices which translate between different telecoms signals, and as such must sit outside of the firewall. It is also likely that the only kind of logging in place regarding the function of a modem is whether the connection is up or down, so a stealthy actor, or pre-positioning for a destructive attack could go unnoticed.

4.7 Microsoft 11 to deprecate NTLM and VBScript, eventually

Microsoft has announced that they will be deprecating NTLM and VBScript. NTLM (technically NTLM v2) is an old and insecure authentication method which stores and communicates passwords in a weakly encrypted format. Attackers have for some time been able to derive the password from this encrypted format, as well as simply stealing the encrypted password and using it to authenticate in what is known as a pass-the-hash attack. VBScript is a very old programming language used for Windows automation and Microsoft Office Macros, which has been constantly used, abused, and attacked by attackers. Deprecation does seem to be good news, however it will be a number of years before these items are actually removed and unavailable in Windows installs.

WithSecure Insight

It is always good news when security increases, and with these announcements Microsoft have essentially stated their intention to increase the security and reduce the attack surface of their operating systems through two specific changes. Initially this will provide the option for organizations to opt-out of NTLM and VBScript, then they will become opt-in, then finally they will be removed altogether. Hopefully this timeline will give organizations which are still running legacy systems the time they need to update or migrate them, however there is always the concern that if they do not have the technical capacity to perform that migration, they could simply end up even more firmly tied to their legacy, insecure systems.

4.8 Apple device geolocation API leaks up-to-date whereabouts of hundreds of millions of devices

In a fascinating study by researchers at the University of Maryland, which was reported by Brian Krebs, it has been found that the highly verbose nature of the Apple geolocation API allows automated queries to pull back enough information to track hundreds of millions of individual Wi-Fi access points. The researchers demonstrated this functionality by identifying Starlink devices used on the frontlines of the war in Ukraine, identifying devices which were previously present in Russia, and devices that were previously present in Western Ukraine, and they were also able to identify access points migrating around the world more generally. They raise the point that this could endanger survivors of domestic violence, or refugees fleeing oppressive regimes. In response Apple have implemented the ability to opt-out of their geolocation database by appending “_nomap” to the end of a Wi-Fi network name (SSID), but with any opt out, public awareness and uptake is likely to be very low. At least there is now a way to opt out of this database.

WithSecure Insight

This is a really interesting piece of research, which gives an insight into how the Apple geolocation API functions, and how it can be abused. Interestingly, Apple choose to return information on a large number of Wi-Fi networks in response to a query, enabling the local Apple device to do the processing to actually work out where it is. By contrast, Google works out the location at the server side, then returns this to the querying device. As such, it seems that the flaw in Apple’s API which enables this mass enumeration may have been an active choice on the part of Apple to protect the privacy of the device making the query, as the location of that device is not stored on Apple’s servers. Unfortunately, that choice to improve the privacy of the 1st party device has had a serious knock-on impact on 3rd party devices.

5 AI

5.1 US proposal for new type of National Vulnerability Database focused on AI

Recognizing that AI vulnerabilities can be a very different thing to software vulnerabilities, the US government have put forth a proposal to set up a new type of National Vulnerability Database that will be specifically concerned with AI vulnerabilities.

WithSecure Insight

While traditional CVEs are essentially specific errors in specific lines of code or combinations of software, an AI vulnerability could be a set of general steps and prompts that can modify the behavior of an AI in an unwanted way, an unintended quirk of the training data set, or unintended situations that an AI can be maneuvered into which can force it outside of its configured guardrails.

5.2 Criminal use of AI growing, but slowly

Researchers at Trend Micro have looked into use of AI by attackers/criminals, as well as by defenders, and concluded that attackers are lagging behind defenders when it comes to implementing AI solutions. They identified only one claimed “criminal” LLM, and a growing number of jailbreaking services for accessing legitimate LLMs. As such, it appears that criminals are mostly focusing on using mainstream products rather than developing their own, which does rather limit the uses to which they can put AI.

WithSecure Insight

We have previously said that AI is more of an efficiency gain than a cyber super-weapon, even if sometimes that efficiency gain is quite drastic. In this research Trend Micro echo something that we have observed in the past, which is that attackers prefer to slowly evolve instead of implementing sudden radical change, often only modifying their behavior under the evolutionary pressure of the cyber security defensive landscape. As such, while their traditional methods are working for them, there is little motive for them to invest effort into AI.

5.3 LLMJacking – a new type of attack

During a recent incident Sysdig observed attackers steal cloud credentials. The attacker then logged into the cloud provider with these credentials and accessed a cloud local hosted LLM instance. All major cloud service providers now offer the ability to host cloud local LLMs from various providers, however this must be enabled by for the account first. Once enabled, new LLM instances can be created with a single command line. Sysdig were able to retrieve the script that was being used in the attack and found that it checks a target cloud environment to see if any one of 10 different LLM services are enabled, what if any quotas have been set, and what the logging configuration is. This script also made reference to OAI reverse proxy, the use of which would enable the attacker to provide proxied access to a fleet of compromised LLMs, without revealing the credentials or hosting environments to the users. Sysdig theorize that with such a set up attackers could sell access to these LLMs to other malicious actors, and that this type of LLMJacking attack could cost victims up to $46,000 per day.

WithSecure Insight

If something has value then financially motivated attackers have a motivation to try to steal it, and cloud compute has a value that is set by the cloud service providers who are selling it. LLMJacking is yet another way that cloud compute can be stolen, enabling the attacker to extract value while somebody else receives the bill.

5.4 AI red team tooling does weeks of reconnaissance in hours

IBM X-Force have reported that by leveraging a generative AI based tool during a red-team engagement they were able to automate what they estimate to be several weeks of reconnaissance and intelligence gathering into a matter of hours. While their AI tool does not replace pen-testers, they state that it has demonstrated that it can very efficiently perform the simpler, data processing tasks that would otherwise take up the time of skilled professionals, freeing them up to spend more time on other, more valuable activities.

WithSecure Insight

Similarly to the previous story on criminal use of AI, here we can see details of an efficiency gain. In this case it is a drastic efficiency increase of roughly 20x over, however this story does have a bit of a marketing bent to it, and we don't actually know how long it would have taken to achieve the same results in a traditional fashion. Even if the increase is overstated, a 5-10-fold efficiency increase in a process is still very impressive.

5.5 Microsoft announce new AI Recall feature

Microsoft have announced a new Windows feature named Recall which has caused a lot of concern in cybersecurity circles. "Recall uses Copilot+ PC advanced processing capabilities to take images of your active screen every few seconds," Microsoft says on its website. "The snapshots are encrypted and saved on your PC's hard drive. You can use Recall to locate the content you have viewed on your PC using search or on a timeline bar that allows you to scroll through your snapshots.", it also uses an AI feature to transcribe and translate speech from videos and video conferences.

WithSecure Insight

While Microsoft claim there are "no security implications" we remain unconvinced. It seems that this feature could give an attacker who has compromised a user account access to anything that user has previously done. It may be that this feature is intended as an aide for users with short term memory issues, as in those cases this sort of regular snapshot has been shown to help recall. If so, and this is an accessibility feature that is available to the small proportion of users who might need it, that sounds great. However, if this is rolled out to all windows users, this could be the next big thing for attackers, providing access to a whole treasure trove of historic, valuable information.

6 Threat data highlights

6.1 Exploits

In WithSecure exploit detection data there is a 10x rise in a 2012 Windows media player Crafted midi file RCE, and some other smaller rises in Microsoft office RCEs. A 2022 Apple OS (i.e. it seems to affect all Apple operating systems) RCE as kernel has also seen a sharp rise, from 12 to 84 detections:

A 2006 Office VBA Macro RCE has seen a very large drop, from 5,500 to 2,500, and the 2023 WinRAR RCE has dropped from 408 to 11, a very significant drop:

Figure 1: WS Detections - CVE Exploits - All - Head

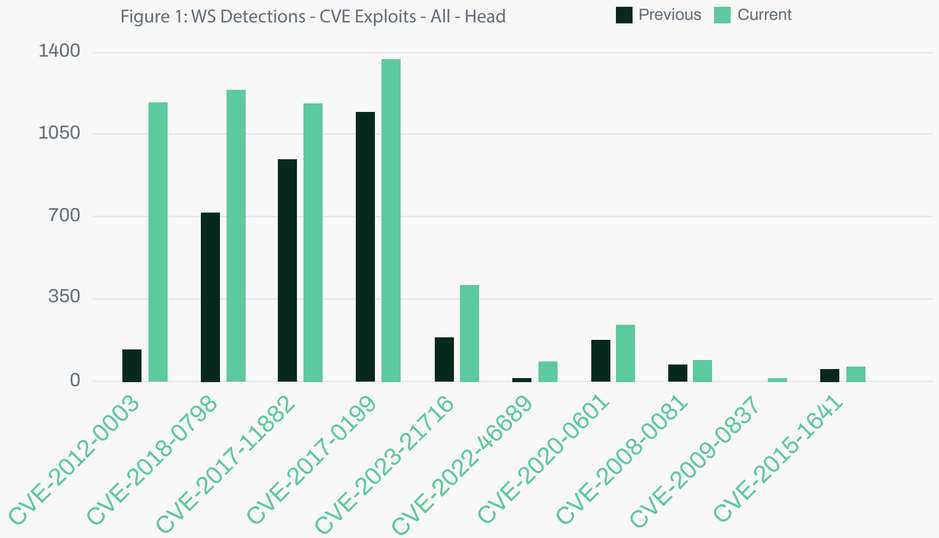
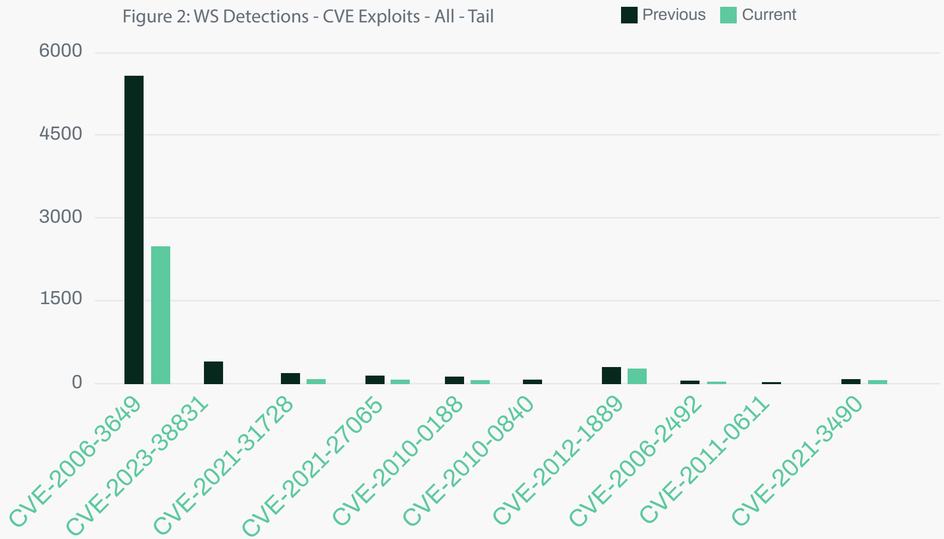


Figure 2: WS Detections - CVE Exploits - All - Tail



Looking at only 2023/24 CVE exploit detections we see that the only increase is in the 2023 Microsoft Word RTF RCE, the 2023 Outlook email notification sound NTLM hash leak vulnerability has dropped slightly, while the previously mentioned 2023 WinRAR vulnerability takes the bottom place with the biggest drop:

The new detections this month are all in very small numbers spread across various older CVEs, with no significant change to mention, though of course the lack of any significant new detections in the data is itself news:

Figure 3: WS Detections - CVE Exploits - 2023/24 - Head

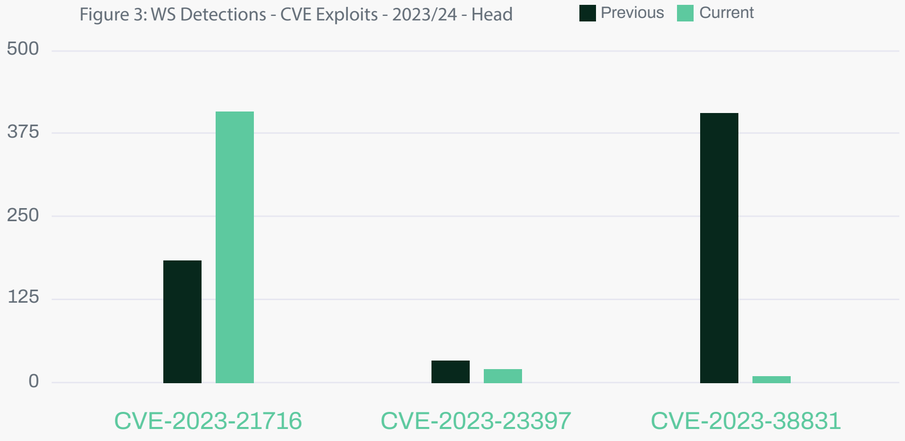
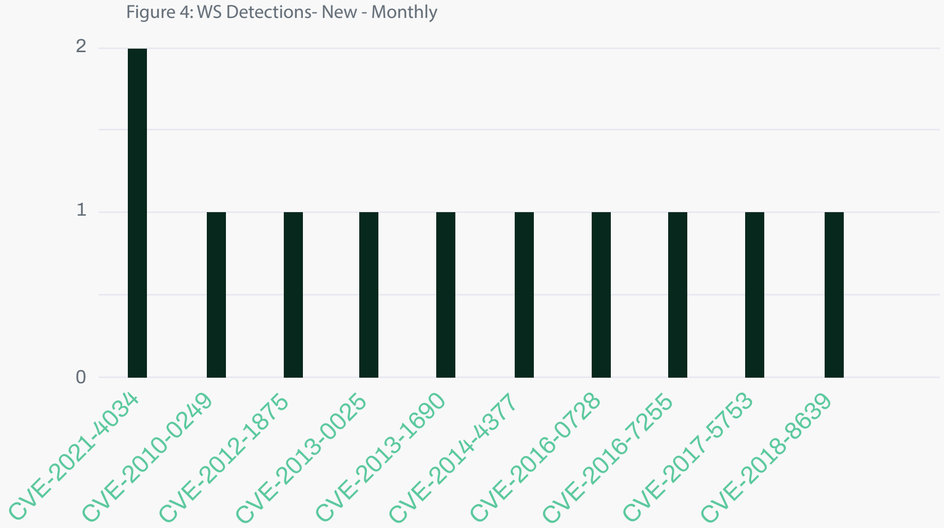


Figure 4: WS Detections- New - Monthly



In VirusTotal 2023/2024 exploit detections, the first-place exploit on the graph is a patch bypass for Windows SmartScreen bypass using .URL files, which has roughly doubled. In second place is a 2024 Ivanti Connect Secure Auth bypass that has risen from 5 detections to 90. At third place is the Windows Authentication privesc vulnerability which has risen from 0 to 46 detections. This was only disclosed in April, so it is not unexpected that it had 0 detections in that month. After all, both detections and exploits take time to write and deploy. However, it has jumped to 46 detections straight away this month. From 4th place onwards there are also increased detections of the 2022 LibWebP RCE exploit, 2023 Confluence administrator account creation, and the 2023 Outlook custom email notification NTLM hash leak vulnerability. That contrasts with WithSecure data, which saw the Outlook vuln drop this month:

Interestingly, while a 2024 patch bypass for 2023 the Windows .URL SmartScreen vulnerability was the biggest increase in the previous graph, the original vulnerability is the biggest decrease in this one, dropping from 2,414 to 591. A similarly large drop was seen in the 2023 Windows MSHTML privesc vulnerability in second place. In third place the 2023 Windows WinSock privesc has dropped from 816 to 24. There are several 2024 CVEs in the graph, interestingly the bottom entry in the graph is a Windows kernel privilege escalation that was added to the KEV in March 2024, however this month it has dropped from 10 detections to 0. This may be because this vulnerability allows privilege escalation from admin to kernel, and only on systems with HVCI enabled, which likely limits its utility to attackers:

Figure 5: VirusTotal 2023/24 CVE Exploit Detections - Head

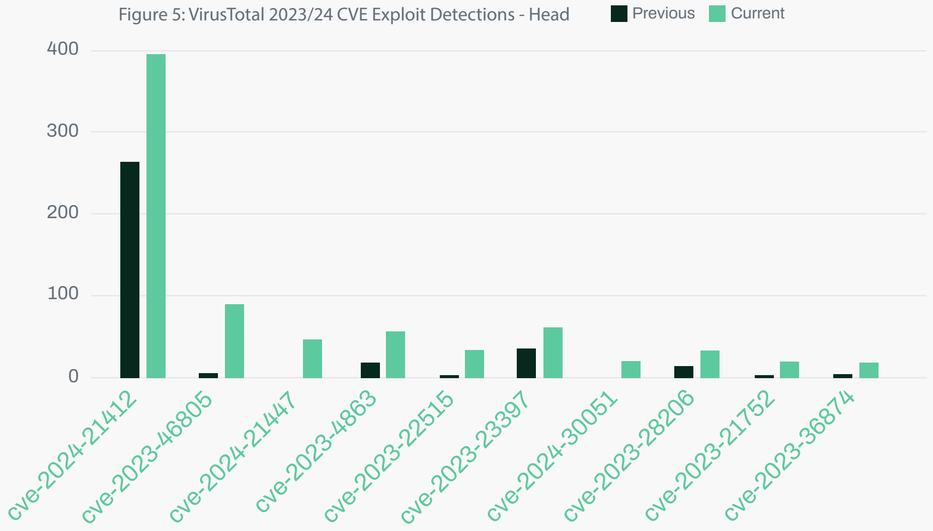
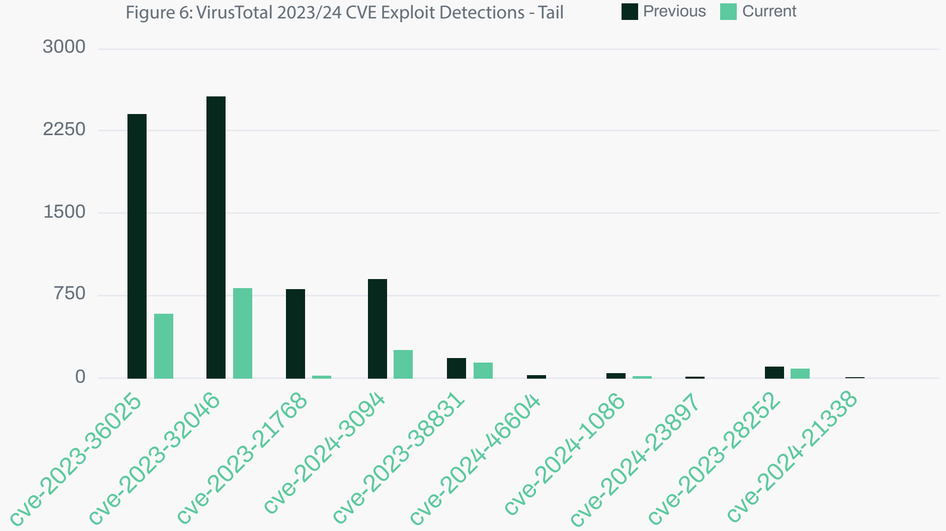


Figure 6: VirusTotal 2023/24 CVE Exploit Detections - Tail



In all VirusTotal exploit detections the top three places are all Microsoft Equation Editor RCEs, which have each seen a roughly 100% rise. As ever, it is possible that these detections are each being triggered by the same files, but it is still a significant rise. In the middle of the graph is the 2017 Huawei router vulnerability which we looked at in more detail last month. We can see that it's use is still growing, but only by around 50% this month. Further down the graph is actually the most detected exploit, a 2016 SQUID DOS vulnerability, which has seen a 10% increase this month. The last two entries on the graph are old ICMP Denial of Service exploits, each detection shows identical numbers so much like last month, this is almost certainly two exploit detections which trigger off a single exploit:

Finally, looking at which exploit detections have fallen in the VirusTotal data, a 2016 DES/Triple DES birthday attack shows the biggest drop at the top of the graph, which is slightly unusual to see, as one would hope DES or Triple DES would not still be in use anywhere. The rest of the graph is made up of either 2023/24 vulnerabilities which were included in the 2023/24 specific VirusTotal graph above, or small fluctuations in older exploits without any particular overarching theme to speak of:

Figure 7: VirusTotal CVE Exploit Detections - All - Head

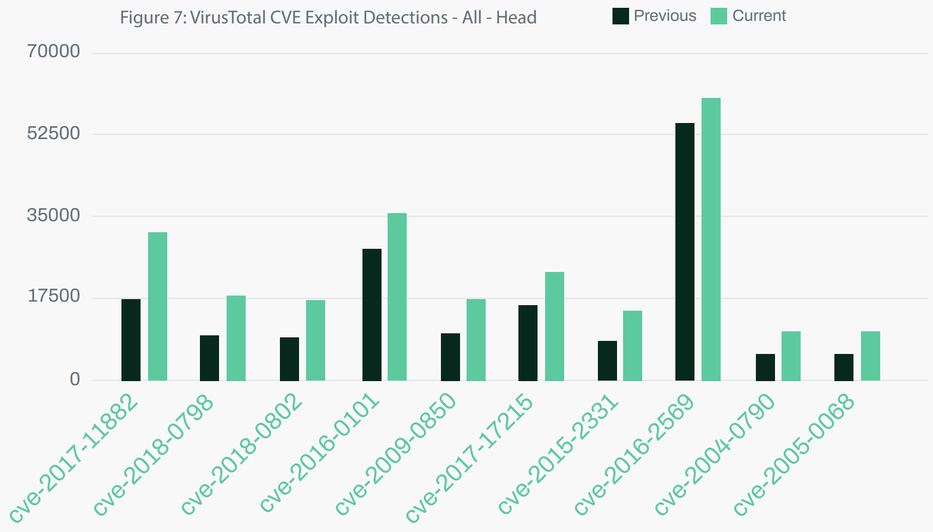
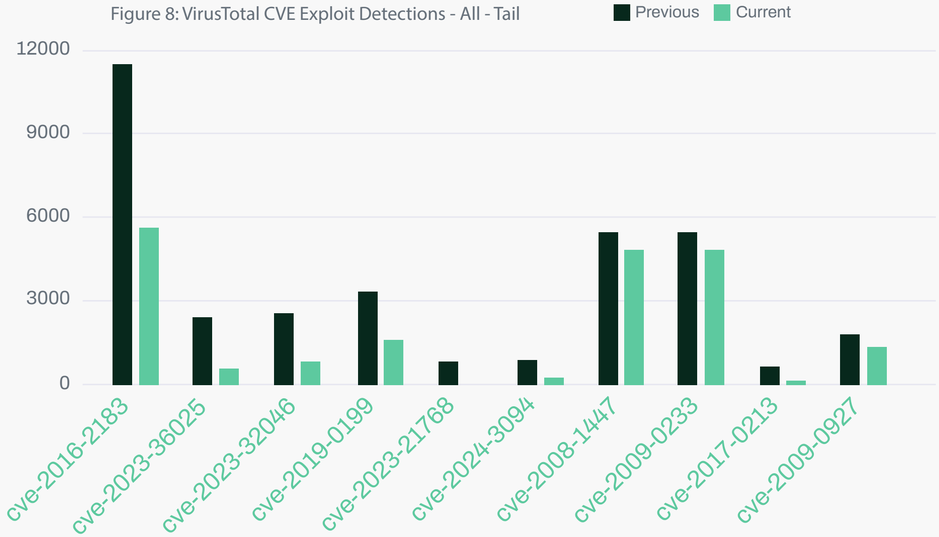


Figure 8: VirusTotal CVE Exploit Detections - All - Tail



6.2 Newly exploited vulnerabilities

Looking at the additions to the KEV this month, we can see the CrushFTP and Cisco ASA zero-days that we discuss this month.

CVE ID	Vendor	Product	Vulnerability	Date added	Description
CVE-2023-7028	GitLab	GitLab CE/EE	GitLab Community and Enterprise Editions Improper Access Control Vulnerability	01/05/2024	GitLab Community and Enterprise Editions contain an improper access control vulnerability. This allows an attacker to trigger password reset emails to be sent to an unverified email address to ultimately facilitate an account takeover.
CVE-2024-4671	Google	Chromium	Google Chromium Visuals Use-After-Free Vulnerability	13/05/2024	Google Chromium Visuals contains a use-after-free vulnerability that allows a remote attacker to exploit heap corruption via a crafted HTML page. This vulnerability could affect multiple web browsers that utilize Chromium, including, but not limited to, Google Chrome, Microsoft Edge, and Opera.
CVE-2024-30040	Microsoft	Windows	Microsoft Windows MSHTML Platform Security Feature Bypass Vulnerability	14/05/2024	Microsoft Windows MSHTML Platform contains an unspecified vulnerability that allows for a security feature bypass.
CVE-2024-30051	Microsoft	DWM Core Library	Microsoft DWM Core Library Privilege Escalation Vulnerability	14/05/2024	Microsoft DWM Core Library contains a privilege escalation vulnerability that allows an attacker to gain SYSTEM privileges.
CVE-2024-4761	Google	Chromium Visuals	Google Chromium V8 Out-of-Bounds Memory Write Vulnerability	16/05/2024	Google Chromium V8 Engine contains an unspecified out-of-bounds memory write vulnerability via a crafted HTML page. This vulnerability could affect multiple web browsers that utilize Chromium, including, but not limited to, Google Chrome, Microsoft Edge, and Opera.
CVE-2021-40655	D-Link	DIR-605 Router	D-Link DIR-605 Router Information Disclosure Vulnerability	16/05/2024	D-Link DIR-605 routers contain an information disclosure vulnerability that allows attackers to obtain a username and password by forging a post request to the /getcfg.php page.
CVE-2014-100005	D-Link	DIR-600 Router	D-Link DIR-600 Router Cross-Site Request Forgery (CSRF) Vulnerability	16/05/2024	D-Link DIR-600 routers contain a cross-site request forgery (CSRF) vulnerability that allows an attacker to change router configurations by hijacking an existing administrator session.
CVE-2024-4947	Google	Chromium V8	Google Chromium V8 Type Confusion Vulnerability	20/05/2024	Google Chromium V8 contains a type confusion vulnerability that allows a remote attacker to execute code via a crafted HTML page.
CVE-2023-43208	NextGen Healthcare	Mirth Connect	NextGen Healthcare Mirth Connect Deserialization of Untrusted Data Vulnerability	20/05/2024	NextGen Healthcare Mirth Connect contains a deserialization of untrusted data vulnerability that allows for unauthenticated remote code execution via a specially crafted request.
CVE-2020-17519	Apache	Flink	Apache Flink Improper Access Control Vulnerability	23/05/2024	Apache Flink contains an improper access control vulnerability that allows an attacker to read any file on the local filesystem of the JobManager through its REST interface.
CVE-2024-5274	Google	Chromium V8	Google Chromium V8 Type Confusion Vulnerability	28/05/2024	Google Chromium V8 contains a type confusion vulnerability that allows a remote attacker to execute code via a crafted HTML page. This vulnerability could affect multiple web browsers that utilize Chromium, including, but not limited to, Google Chrome, Microsoft Edge, and Opera.
CVE-2024-4978	Justice AV Solutions	Viewer	Justice AV Solutions (JAVS) Viewer Installer Embedded Malicious Code Vulnerability	29/05/2024	Justice AV Solutions (JAVS) Viewer installer contains a malicious version of ffmpeg.exe, named fffmpeg.exe (SHA256: 421a4ad2615941b177b6ec4ab5e239c14e62af2ab07c6df1741e2a62223223c4). When run, this creates a backdoor connection to a malicious C2 server.
CVE-2024-1086	Linux	Kernel	Linux Kernel Use-After-Free Vulnerability	30/05/2024	Linux kernel contains a use-after-free vulnerability in the netfilter: nf_tables component that allows an attacker to achieve local privilege escalation.
CVE-2024-24919	Check Point	Quantum Security Gateways	Check Point Quantum Security Gateways Information Disclosure Vulnerability	30/05/2024	Check Point Quantum Security Gateways contain an unspecified information disclosure vulnerability. The vulnerability potentially allows an attacker to access information on Gateways connected to the internet, with IPSec VPN, Remote Access VPN or Mobile Access enabled. This issue affects several product lines from Check Point, including CloudGuard Network, Quantum Scalable Chassis, Quantum Security Gateways, and Quantum Spark Appliances.

7 Research highlights

7.1 Generative AI – an attacker's view

Research by Tom Taylor-MacLean looking at how hackers are using generative AI to enhance their offensive capabilities, then how we can protect ourselves from these attacks. Consideration is given to both the human and technical elements.

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

Our latest reports: Threat-Research