Threat Highlight Report

March 2024

WITH secure

Contents

Foreword

This month the flood of zero-days which characterized the beginning of 2024 has finally slowed. However, it has unfortunately been followed by disagreement and recrimination between organizations who should really be on the same side. JetBrains and Rapid7 publicly disagreed over the correct way to perform responsible disclosure, while CISA and Ivanti disagreed over whether the detection and remediation tools that Ivanti offer to their ICS customers work correctly. News from the ransomware industry continues to delight defenders as major players BlackCat/ALPHV have closed their operation with a major exit scam carried out against their former affiliates. In combination with the recent Lockbit takedown this seems to have caused a crisis of trust within the Ransomware as a Service industry.

We also cover multiple other interesting and important highlights from the cyber threat landscape, analyze internal WithSecure detection telemetry, and cover WithSecure research into medical technology protocol analysis. This research was released this month alongside the ‘open-sourcing’ of a new protocol analysis tool.

- Stephen Robinson, Senior Threat Intelligence Analyst, WithSecure

1 Monthly highlights

1.1 JetBrains TeamCity vulnerability widely exploited as researchers and developers disagree over responsible disclosure

A patch was issued for JetBrains' CI/CD software, TeamCity, on March the 4th. JetBrains then posted an advisory stating that two critical vulnerabilities were addressed by the patch, CVE-2024-27198 and CVE-2024-27199, and that they could enable an unauthenticated attacker to gain administrative access to the server. They also stated that the vulnerabilities had been identified by researchers at Rapid7, and that within 24 hours Rapid7 would release technical details of the vulnerability and how to exploit them. Shortly after this, Rapid7 then published their own post about the vulnerabilities, stating that they believed JetBrains had released the patch without notifying Rapid7 or publicly disclosing the vulnerabilities. Following this, there appeared to be some public statements from both sides raising concerns with the others' proposed approaches.

Rapid7's approach is based on the fact that as soon as a patch is issued to fix a vulnerability, the vulnerability and how to exploit it is available to anybody who can reverse engineer that patch. Since most IT patching teams don't regularly reverse engineer patches just to see what's there, this can mean that a silently patched vulnerability becomes exploitable to attackers before defenders are aware of it. Therefore, by publicly and transparently giving all details of a vulnerability at the point that it is patched, it ensures that both attackers and defenders have all possible information about it, and so defenders can correctly prioritize their response.

WithSecure Insight

There are clearly differing opinions in how to handle critical vulnerability disclosure, and we do not wish to weigh in with (yet another) opinion, however we do want to highlight that this is (yet another) reminder that exposure and vulnerability management is hard. Critical vulnerabilities on internet facing services are increasingly exploited to compromise ever increasing numbers of enterprise victims (per ransomware statistics).

This back and forth between two organizations who should be on the same side is itself concerning, and to compound this, the vulnerability is now being exploited in the wild. Two days after the patch was issued LeakIX stated that over 1,700 TeamCity servers were still vulnerable, and that mass, automated exploitation appeared to be ongoing, with over 1,400 of those vulnerable servers having been exploited. The exploit has been used to create new administrative users, and on some vulnerable servers upwards of 300 new administrative users with randomized, 8-character account names have been created, a strong indicator that exploitation is being automated.

Because TeamCity is used by software developers as part of their software build and deployment pipeline, every compromised TeamCity server is an opportunity for a supply chain attack against users of that software.

1.2 VMWare vulnerable to chainable CVEs discovered at Tianfu Cup, reported to be a Chinese government exploit gathering exercise

Four vulnerabilities that affect VMWare ESXi, Workstation, and Fusion have been patched by VMWare. These vulnerabilities are CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255. The individual vulnerabilities have a severity rating of Important, but VMWare have noted that combining the different vulnerabilities leads to a Critical severity exploitation chain.

Two of the vulnerabilities (22252 and 22253) are 9.3 CVSS severity sandbox escapes, however they only provide sandbox escapes on Fusion and Workstation. On ESXi they allow code execution from the VM into the VMX sandbox, but not beyond, and so in that context are rated as 8.4 CVSS.

However, another of the vulnerabilities (22254) is a VMX Sandbox escape on ESXi, so this could be chained with the VM escape vulnerabilities to provide full sandbox escape on VMWare ESXi. This is an excellent example that while individual CVEs may have a lower severity, they can be combined/chained together to have a critical impact.

WithSecure Insight

It should be noted that these vulnerabilities were reported by researchers working with the Tianfu Cup Pwn Contest, which reporting on the recent iSoon leaks describes as being used as part of an exploit development and acquisition program for the Chinese government's cyber threat actors. In a similar way, research published way back in 2017 by Recorded Future suggests that the Chinese National Vulnerability Database (CNNVD) is also used to funnel exploitable vulnerabilities into the hands of Chinese state sponsored cyber actors. Most noteworthy is that for the US NVD, high CVSS vulnerabilities are published much more quickly than low CVSS vulnerabilities. By contrast, CNNVD on average publishes high CVSS vulnerabilities much slower than low CVSS, and it shows a statistically unlikely delay around publishing details of vulnerabilities which are being actively exploited by Chinese APT groups.

1.3 CISA and Ivanti disagree about Ivanti ICS security – Who to believe?

On the last day of February, CISA and their Five Eyes (US, UK, Canada, Australia, and New Zealand) partners issued an advisory which stated that Ivanti's ICS Integrity Checker Tool is not sufficient to detect compromise of a device by threat actors, and that research performed by CISA using virtual Ivanti ICS appliances indicated that threat actors could gain root-level persistence which could endure through factory resets on ICS devices. Ivanti rapidly updated a previous statement to disagree with CISA and FVEYs, stating that CISA's persistence method would only be possible in lab conditions, and noting that the persistence method has not been observed in the wild. Ivanti also linked to analysis from Mandiant which stated that it had observed failed attempts, but no successful attempts to maintain persistence through factory resets.

While Ivanti were very emphatic that they are not aware of any successful attempts to persist through factory resets, they did issue a new version of their integrity checker tool to address that part of CISA's criticism. They also changed their advice regarding virtual appliances, stating that in certain situations customers should not factory reset, but instead deploy an entirely new build of the virtual appliance, as factory resets of virtual appliances "have not been consistently successful", meaning that they have been known to fail.

WithSecure Insight

It is unfortunate that as we enter the fourth month of this Ivanti ICS security incident, the status of the incident, and the correct remediation steps for potential victims remains unclear and subject to change. As ever, the advice remains to keep patching, to apply security controls to prevent unwanted or unexpected behavior even from trusted infrastructure, and to pro-actively monitor for any such behavior. It is always easier to prevent a compromise than it is to recover from one.

1.4 Reports of political espionage by China

WithSecure Insight

The UK Deputy Prime Minister made an announcement stating that the August 2021 compromise of the UK Electoral Commission, the body which is responsible for elections in the UK, was carried out by Chinese state sponsored attackers. During this attack it is believed that a significant portion of the database of UK citizens who are allowed to vote was stolen, estimated to include the details of around 40 million registered UK voters. In addition to attributing this attack to China, the UK government stated that a number of UK politicians were also targeted by Chinese state sponsored attackers. The targeted politicians were all members of a parliamentary group which is critical of China. The UK government have sanctioned several Chinese nationals are employees of Wuhan Xiaoruizhi Science and Technology Company Ltd, which they state is the cyber espionage group APT31.

The US government also sanctioned the company alleged to be behind APT31, and issued arrest warrants for the two individuals sanctioned by the UK, along with another five Chinese nationals. Shortly after, the New Zealand government issued a statement that the parliamentary counsel office and parliamentary service was also targeted by China in 2021, in that case by APT40. The following day the Finnish police made a statement attributing cyber-attacks on the Finnish parliament in 2020 and 2021 to APT31.

It is often taken as a given that espionage between geopolitical powers happens all the time, and situations like this are often reported upon with a vicarious pleasure. Compared to a ransomware attack or financially motivated crimes there may not be much of an immediate impact, these attacks did after all occur two to three years ago. However, it is interesting to consider what the impact of these attacks may have been. In the case of the UK Electoral Commission hack, it may at first look like an attempt to influence election results, however it is also possible that the attack was carried out with the intention of stealing the voter database, a source of high quality, stringently verified personal details of tens of millions of UK citizens. In our modern world of big data and data driven insights, large quantities of accurate data on individuals could have any number of uses.

2 Ransomware: Trends and notable reports

2.1 The numbers

Throughout March 2024 numbers of new victims posted to a ransomware breach site have stayed relatively stable at 420 compared to 434 in February. Interestingly many victims have been re-uploaded during this month (not counted) and we do not know why – possibly a symptom of affiliate reorganization following Blackcat's exit scam, or LE action on Lockbit.

Numbers of victims posted to Lockbit's site have remain roughly consistent with last month, however upon closer inspection it appears that many of Lockbit's victims have been reposted from older posts. If we filter these out, new victims appear to have more than halved, from 107 to 49. Lockbit remains the most active actor, but the margin is greatly reduced. PLAY is the second most active group, filling the void left by BlackCat/AlphV after their exit scam where numbers have increased from 4 (Jan), 26 (Feb) to 46 (March).

The list of 'new' groups observed this year (where their leak sites are parseable) has increased from 11 (Jan-Feb) to 17 (Jan – March). Of these, worth noting is 'Red Ransomware' which posted 12 victims, putting it 11th place in this month's list. 'Kill Security', 'Donex' and 'Dispossessor' have posted 5 victims each.

Ransomware	Feb '24	March '24	Change
Insane	0	0	0
3AM	6	2	-4
8BASE	23	17	-6
Abyss	6	5	-1
Akira	16	19	3
Alphv (BlackCat)	45	8	-37
BianLian	21	17	-4
BiteMe	-	1	1
BlackBasta	24	35	11
Blackbyte	6	1	-5
Blackout	2	1	-1
Blacksuit	0	8	8
Cactus	7	10	3
CHCC Leak	-	1	1
CiphBit	1	0	-1
CL0P	0	4	4
Cloak	3	8	5
Cloak Ransomware	0	0	0
CUBA	1	0	-1
Data Leak	5	1	-4
Defray777	0	5	5
Dispossessor	-	5	5
Donex	-	5	5
Donut Leaks	4	2	-2
DragonForce	5	6	1
Dunghill Leak (News)	2	0	-2
Everest	1	3	2
HelloGookie	-	4	4
Hunters International	33	17	-16
INC Ransom	4	13	9
Kill Security	-	5	5
Knight	5	0	-5
LockBit	107	49	-58
Mallox	0	3	3
Medusa	14	27	13
Meow	6	2	-4
Mogilevich	5	4	-1
Monti	2	0	-2
MyData	1	1	0
Play	26	46	20
Qilin	11	10	-1
RA Group	0	10	10
Ransomed	3	0	-3
Ransomhouse	7	0	-7
RansomHub	7	18	11
Red Ransomware	-	12	12
Rhysida	4	5	1
slug	0	0	0
Snatch	2	13	11
Stormous	6	10	4
Trigona	4	6	2
Trisec	3	0	-3
Underground	6	2	-4

2.2 ALPHV bow out with $22 million exit scam

Recently the US healthcare/pharmacy organization Change Healthcare suffered an ALPHV ransomware attack which had significant real-world impacts for healthcare across the country. Several weeks after this attack, a person claiming to be the ALPHV affiliate who performed the Change Healthcare cyberattack posted on a Russian language cybercrime forum. They stated that while Change Healthcare had paid the $22 million ransom to ALPHV to prevent stolen data being leaked, ALPHV had not passed on the share that was owed to the affiliate. Instead, they suspended the affiliate's account and kept the money. Change Healthcare has not confirmed that they paid such a ransom, however a cryptocurrency address which researchers have previously linked to ALPHV did receive a single, $22 million payment. An apparent member of the core ALPHV brand posted to the same cybercrime forum stating that they were shutting down the group and had already found a buyer for their ransomware source code. They also stated that they "got screwed by the feds", and ALPHV's website was replaced with a law enforcement takedown notice. However, researchers rapidly noted that the takedown notice was just a screenshot of the previous takedown notice from when ALPHV were last taken down by law enforcement in 2023.

WithSecure Insight

Looking at the sequence of events that have been reported, the most plausible explanation is that ALPHV have performed an exit scam, claiming to have been taken down by law enforcement and forced to shutter by forces beyond their control, when actually they've just run off with a big pile of stolen money which they in turn had stolen from one of their fellow criminals. Truly, there is no honor among thieves.

Unfortunately for Change Healthcare, while it is highly likely that they did pay a very large ransom to avoid their data being leaked, the cybercrime forum member who claims to be the affiliate who performed the attack has stated that they still have the stolen data. As such, it is entirely possible that they will either attempt to re-extort Change Healthcare or find a buyer for the data.

An important lesson from this is that paying cybercriminals to do something based on trust is not a good idea. Paying for a decryptor is extremely risky, however at least then the victim/payee can verify that the data has indeed been decrypted. Paying a cybercriminal to delete stolen data is even more risky, as there is no way to ensure that the data has actually been deleted.

2.3 Crisis of Trust in RaaS industry after Lockbit takedown and ALPHV exit scam

A recent report from researchers at GuidePoint Security looks into the ransomware ecosystem and gives insight into how it has responded to the recent shockwaves of the Lockbit and ALPHV takedowns, and the recent ALPHV exit scam. Interestingly, a number of smaller/newer ransomware brands such as Medusa, RansomHub, and cloak appear to be trying to attract affiliate operators who have been directly affected or discouraged by the Lockbit takedown and ALPHV exit scam. Medusa are offering generous profit-sharing percentages, with up to 90% going to the affiliates, stating that they would accept non-Russian speakers. RansomHub, on the other hand, are up ending the RaaS orthodoxy by letting affiliates accept payment from the victims directly, before then sending a share to the brand. This appears to be a clear attempt to reassure those who may have been spooked by ALPHV's exit scam, which was only able to occur because the payment from victims first went to crypto-wallets controlled by ALPHV, before ALPHV then sent the affiliate's share on to their own crypto-wallet. Finally, while Cloak's offering is not as radical as the other two groups, they still offer an 85% profit share to affiliates, with no initial payment needed to become an affiliate.

WithSecure Insight

These relatively dramatic offerings could be taken as an indication that while the law enforcement takedown of Lockbit and ALPHV may not have been immediately and directly able to eradicate the brands, they have applied great pressure to the ransomware industry, and it would appear that trust in Ransomware as a Service brands by their affiliates is at a very low ebb. From the perspective of a defender this is ideal, because as stated in last month's report, if cybercriminals do not trust each other, and do not collaborate with each other, it is a very reasonable assumption that they will be less effective, less efficient, and easier to defend against.

2.4 FBI report that ransomware attacks have increased against critical infrastructure

The FBI issued their 2023 report on cybercrime this month, which included statistics on various types of cybercrime, including ransomware. Their numbers (based on incidents reported to them by victims) show that compared to 2022 there was an 18% increase in reported ransomware attacks to 2,825, and a 74% increase in losses due to ransomware attacks, NB: do note that is losses incurred, not ransoms paid.

An even more concerning statistic is that of the 2,825 reported attacks, 1,193 were against critical infrastructure organizations, an increase of 37% on the previous year. The reported losses to ransomware rose 74% from $34.3 million to $59.6 million, which is a relatively small amount when compared to the $4.57 billion lost to investment fraud in 2023. The majority of investment fraud was investment fraud which referenced cryptocurrency, which made up $3.96 billion of the reported losses. This is a 38% increase in investment fraud losses on 2022, and a 53% increase in cryptocurrency investment fraud.

WithSecure Insight

From these numbers one could draw the conclusion that ransomware profits are growing faster than investment fraud profits, however, do remember that this is an extremely complicated space and these statistics do have a lot of caveats that may mean there may be little value in making comparisons between them.

2.5 Research suggests mass exploitation has replaced botnets as the primary ransomware infection vector

Research published by Symantec this month suggests that the primary infection vector for Ransomware has changed from botnets to vulnerability exploitation, an interesting and significant finding if true. Symantec draw this conclusion from 126 ransomware intrusions they investigated, which found that in the majority of those incidents the infection vector for the attack was mass exploitation. While they do not provide a numerical breakdown, they state that the likely infection vectors in recent ransomware attacks they investigated included vulnerabilities in ZOHO ManageEngine, Microsoft Exchange, Citrix Netscaler ADC (Citrix Bleed), and Cisco ASA firewalls.

WithSecure Insight

We have covered the threat from actors exploiting edge services and need for exposure management so much already in this, and previous, reports and do not see the need to do so again here.

2.6 British Library issues public report with full details of ransomware attack and recovery

In October 2023 the British Library suffered a significant ransomware attack by the Rhysida ransomware brand, a rebrand of Vice Society. Now they have made public their lessons learned document, including details of the cause and impact of the attack, their recovery process, and their future risk assessment. This is an admirable work of transparency, as well as a highly educational and interesting record of the full lifecycle of a ransomware attack.

3 Other notable highlights in brief

3.1 IoT – Exactly as secure as you expect it to be

This month research was published on several significant IoT vulnerabilities. Firstly, a team of security researchers published a vulnerability in the Saflok brand of RFID-based keycard locks which are used in an estimated 3 million hotel doors in 131 countries. As well as the number of doors affected, a significant issue with this vulnerability is how long it could take to patch. The manufacturers have been aware of and addressing the vulnerability for a year, and only 36% of locks have so far been updated, with the researchers predicting that it could take months or years until all the locks are patched.

CISA also added CVE-2019-7256 (CVSS 10.0) in the Nice Linear eMerge E3-Series operating system to the KEV. This OS is used in a brand of physical access control servers, and the CVE allows remote code execution. While the vulnerability was discovered and disclosed in May 2019, it was only patched by Nice this month, and is known to have been under exploitation by threat actors since as early as February 2024.

Finally, rounding off a trio of IoT related vulnerabilities which could have real world impact, a paper was presented at the fascinating sounding 2024 Network and Distributed System Security Symposium which describes vulnerabilities discovered in a significant yet unspecified proportion of Electronic Logging Devices (ELDs). The vulnerabilities could enable an attacker within Bluetooth or Wi-fi range to remotely control a vehicle, manipulate logged data, or infect it with worming malware which can spread between vehicles.

WithSecure Insight

This is particularly concerning as ELDs are required to be installed in US commercial heavy goods vehicles. The researchers describe how they were able to remotely compromise an ELD in a real-world simulation via an unsecured API which permits over the air firmware updates. The API was accessible via weakly secured default Bluetooth or Wifi connections, and the researchers were able to remotely control the vehicle, causing it to slow down. They also illustrate that it would be entirely possible to create a malware which would autonomously spread between vehicles within wireless communication range, and which could then be configured to remotely control all affected vehicles at a specified time.

3.2 Fortinet enterprise management software under exploitation

Researchers have released a Proof of Concept POC) for critical vulnerability CVE-2023-48788 in Fortinet FortiClient Enterprise Management Server one week after it was patched. The vulnerability is a SQL injection which impacts versions 7.0 and 7.2, allowing unauthenticated privileged RCE, and Fortinet have updated their security advisory to state that it is being exploited in the wild. Enterprise Management Server are very sensitive devices within a corporate network, as they typically can remotely manage many other devices. As such, ideally, FortiClient EMS servers would not be Internet connected, but even so, if an attacker is able to gain a foot hold on a network and then access an EMS server it could have a significant impact across the network.

3.3 Millions of records exposed by misconfigured sites using Google Firebase

Researchers have found at least 900 websites built with Google backend cloud database service Firebase to be misconfigured, leaving more than 125 million user records publicly accessible. Data discovered by the researchers includes 27 million billing information records, 20 million plaintext passwords, 85 million names and 106 million email addresses.

3.4 Analysis issues at key vulnerability database, NVD

Researchers have raised concerns that the US National Vulnerability Database (NVD) has recently stopped enriching their feed of published CVEs with the additional analysis which is relied upon by many companies for security operations and vulnerability research. Almost no CVEs have been published with additional analysis since February 12th, and 42% of the >6,000 vulnerabilities published in 2024 have no analysis in the NVD database. On the 15th of February NIST published a banner on the NVD website stating that they were attempting to address challenges in the NVD program, which would introduce temporary analysis delays. It is likely that few people reading that message would have expected such a drastic impact.

3.5 EU passes AI Act to attempt to regulate AI and LLM technology

The EU Parliament has passed the 'AI Act' with roughly 80% of votes in favor. The stated aims of the act are to protect fundamental rights, democracy, the rule of law, and environmental sustainability from high-risk AI, whilst boosting innovation. The act classifies AI systems according to the harm they could do if they fail to work as intended, and any systems which fall under the highest tier of risk would be "prohibited". The act also forbids social scoring, predictive policing, and biometric categorization systems based on sensitive characteristics. Opposition to the bill has warned that the rules could hamper domestic companies competing with companies in the US and China, however looking at the list of forbidden systems, it does seem like that might be a price worth paying.

3.6 Database of 2fa codes for Facebook, Google and TikTok was left exposed to the Internet

TYX International is a manufacturer of mobile/cellular networking equipment that also provides SMS routing services, claiming to send millions of text messages a day. A researcher who specializes in discovering exposed databases on the internet found that an internal YX international database was exposed to the Internet, although because it was not clear who the database belonged to, the researcher shared details of the database with TechCrunch to try to identify the owner.

The database contained the contents of text messages sent to users, including one-time passcodes and password reset links sent by companies such as Meta, WhatsApp, Google and TikTok. The researchers were eventually able to identify internal YX International email addresses and passwords and contacted the company to inform them of the issue. Shortly after the database went offline, and YX International stated that they had sealed the vulnerability, but that there were no access logs for the server in question, so there was no way to tell if anyone other than the security researchers had accessed the database and its contents.

For some time now it has been the case that while multifactor authentication is strongly recommended, authentication apps have been preferred over SMS due to its insecure nature and the prevalence of attacks such as SIM Swapping.

3.7 Study finds 56% year on year increase in number of zero-days in 2023

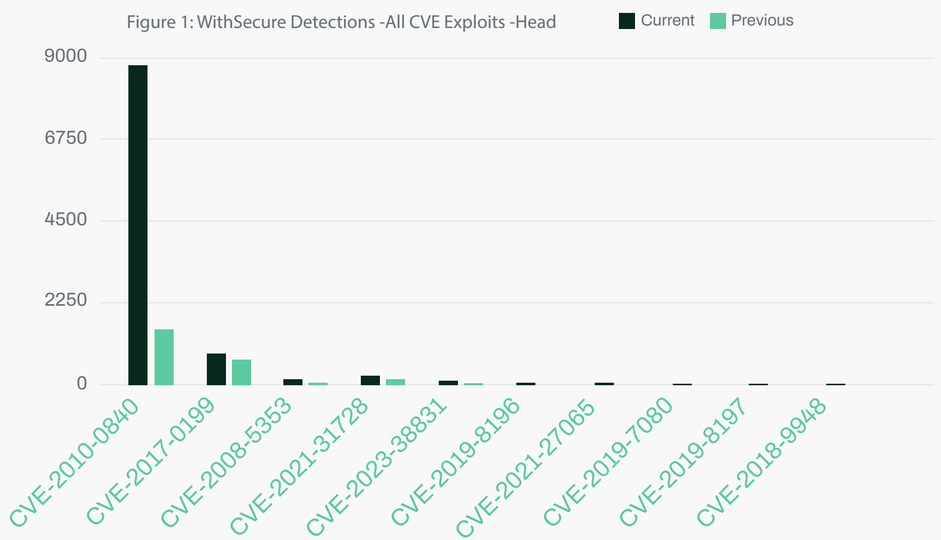
A study by researchers at Google and Mandiant reports that there were 97 zero-days in 2023 compared to 62 in 2022, an increase of 56%. They also found that the number of zero-days affecting enterprise software increased by 64% from 2022, indicating that they are becoming more prevalent more quickly than zero-days as a whole. The researchers attribute this increase to vulnerable security software and infrastructure/ appliances. The researchers also investigated the motivation of the threat actors that zero-days were attributed to and found that 41.4% were attributed to nation state sponsored hackers, with the same number attributed to "commercial spyware vendors", i.e. hackers for hire such as NSO group. The other 17.2% were attributed to financially motivated attackers.

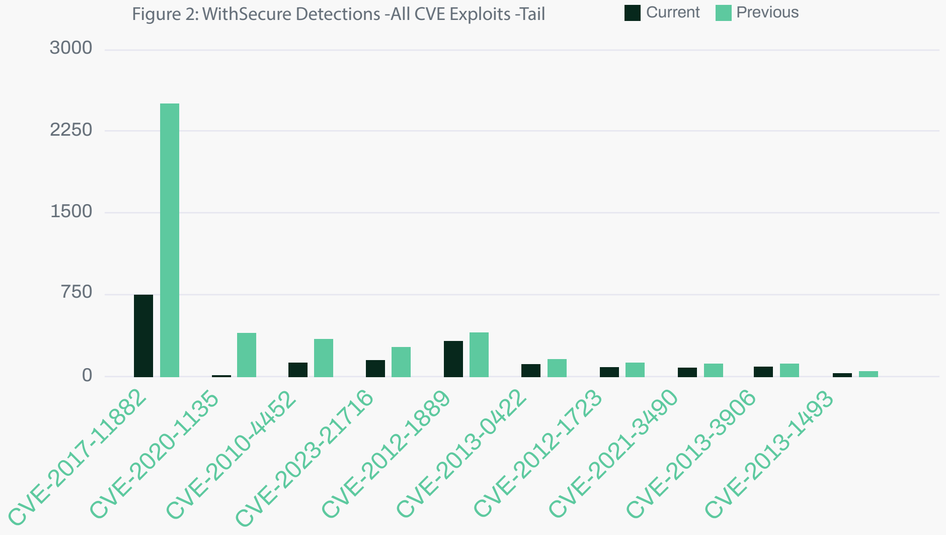
4 Threat data highlights

4.1 Exploits

In WithSecure detection data there has been a huge rise in CVE-2010-0840 (Java 6 RCE) detections. While this is a very old CVE, it was only added to CISA's KEV in May 2022. Of the 10 Exploit detections with the highest month on month increase, three are Adobe Acrobat/Reader vulnerabilities, while one is a Foxit PDF reader vulnerability. While this may suggest that there has been a recent increase in use of malicious PDFs, another possible explanation is that these vulnerabilities could be related, such as being patch bypasses of a single flaw, so it could be that the same files are triggering multiple exploit detection rules.

There has also been a very large drop in exploit detections of CVE-2017-11882 (a Microsoft Office Equation editor vulnerability), first added to the KEV in March 2021. In late 2023 Kaspersky noted that this vulnerability was still under active exploitation, even though patches have been available for many years now. As such, it seems likely that this is a vulnerability that is a regular part of any standard malspam arsenal.





Looking at 2023/24 CVE exploit detections specifically, we see a rise in CVE-2023-38831, the recent WinRAR RCE. This reinforces our assessment last month that this is past its initial surge in use and is now part of the ‘background noise’ of exploitation. The first malware-bourne 2024 CVE detections occur with CVE-2024-21412, which is a Windows .URL file security feature bypass vulnerability. There is also a slight drop in CVE-2023-23397, the Outlook custom notification sound NTLM hash harvesting vulnerability, another one that we believe is now being steadily compromised.

Finally in WithSecure telemetry, new month on month detections (i.e. detections in March for which there were no detections in February). Here we see echoes of the other graphs – The three 2019 CVEs (7080, 8197, and 8195) are Adobe Acrobat/Reader vulnerabilities, as seen and discussed in the top detections, and we also see CVE-2024-12412 (.URL file security bypass).

Figure 3: WithSecure Detections -2023/24 CV Exploits

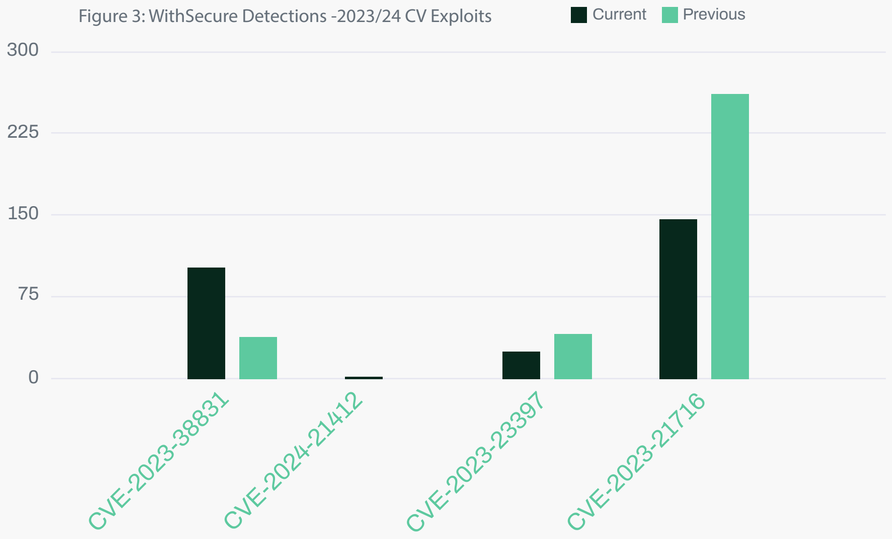
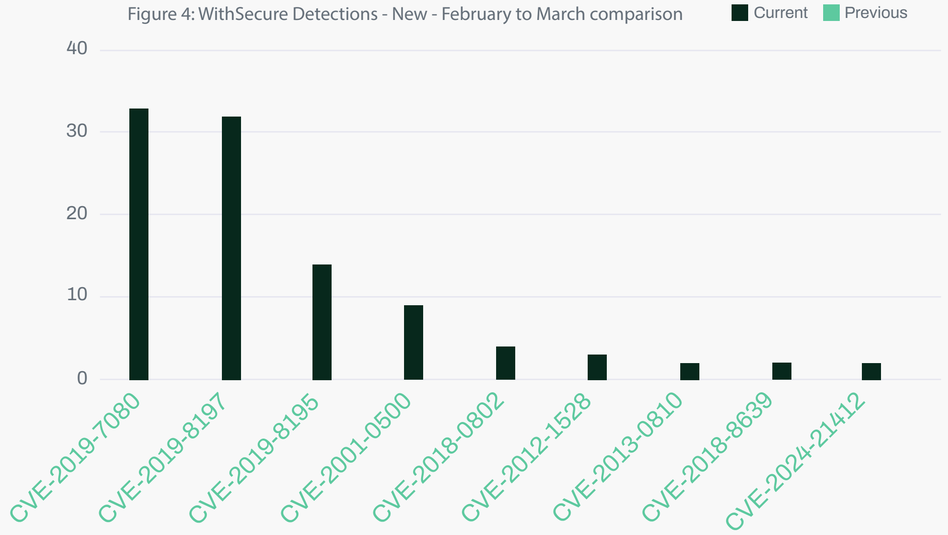


Figure 4: WithSecure Detections - New - February to March comparison



In VirusTotal exploit detections there are large increases in CVE-2023-36025 (Another .URL file security bypass) and CVE-2023-32046, a Windows MSHTML PrivEsc vulnerability. While much smaller in volume, it is interesting to see CVE-2023-3094 detections, which is the XZ library backdoor, and CVE-2023-32434 again, the Mac/iOS PrivEsc RCE. The presence of the XZ backdoor highlights that these numbers reflect not only how heavily targeted a CVE is, but also how widely available files using the exploit are, and how interested the users of VirusTotal are in such samples and their detectability.

The majority of these detections are Windows vulnerabilities, but the Veeam credential access/decryption vulnerability CVE-2023-27532 makes the list, as does the GitLab CE/EE path traversal CVE-2023-2825, and Cisco AnyConnect VPN Client update process privesc, CVE-2023-20178. While the number of detections of the Cisco AnyConnect Client vulnerability may not be significant, it is a very interesting vulnerability to read up on if you are not aware of it.

The Ivanti ICS auth bypass, CVE-2023-46805 has dropped significantly from 44 detections to 7, and the JetBrains TeamCity auth bypass RCE from late 2023, CVE-2023-42793, has dropped to 0 this month, but most other detection drops are not particularly significant when you consider that in the previous graph there were changes in detection volumes in the thousands.

The VT data for CVE-2023-23397, the Outlook NTLM hash harvesting vuln mirrors WithSecure's detection data, showing a drop, but with ongoing usage.

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

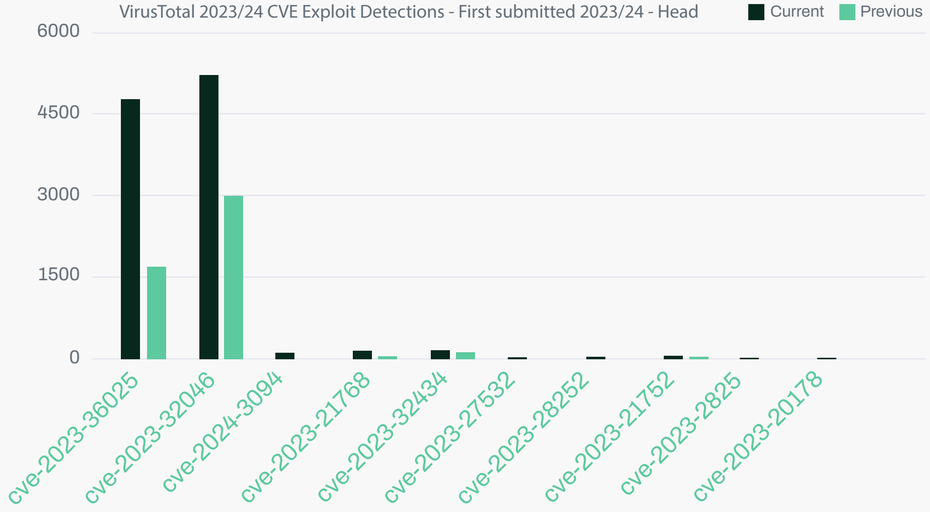
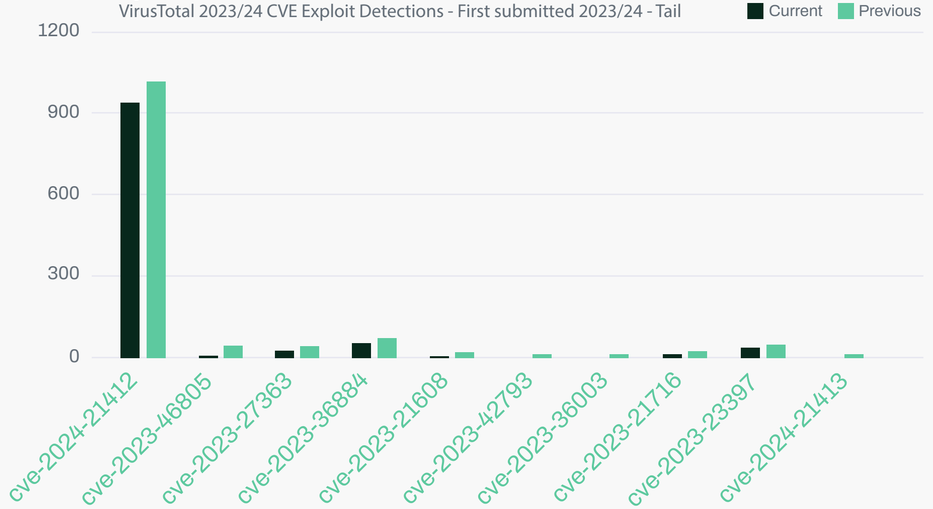


Figure 6:
VirusTotal 2023/24 CVE Exploit Detections - First submitted 2023/24 - Tail



Looking at all exploit detections we can see significant increases in CVE-2016-2569, a SQUID Denial of Service vulnerability, CVE-2016-0101, a Windows Media file parsing RCE, and CVE-2021-1732, a Windows 10 PrivEsc vulnerability that went from 640 detections last month to 12,422 this month. There are 4 different CVEs which target Microsoft Office, 3 of which are Equation Editor RCE vulnerabilities, CVE-2017-11882, CVE-2018-0798, and CVE-2018-0802. '0802 and ‘11882 were also seen in WithSecure telemetry, although there ‘11882 was seen falling, not rising.

At the bottom of the graph are two interesting, niche vulnerabilities. CVE-2019-0199, an Apache Tomcat HTTP/2 denial of service vulnerability, and a Huawei HG532 router unauthenticated RCE. As with any niche vulnerability of this type, making it into the top 10 in this way implies that within that specific ecosystem it must be very prevalent indeed. It is worth noting that in Huawei’s advisory they state that there is no patch, instead there are a set of suggested mitigations.

Looking at detection drop in VT data there is a large drop in CVE-2009-1122 which is an IIS 5.0 auth bypass, and a large drop in CVE-2011-3230 which is an RCE in older Safari versions. The next three vulnerabilities, CVE-2007-3034, CVE-2005-4560, and CVE-2008-2249 are all Windows 2K-2K3 RCE via crafted image file vulnerabilities, and the very similar type and volume does suggest that these may be auth-bypasses or closely related vulnerabilities which are being triggered by the same exploits. This may be a similar situation to the Adobe Acrobat vulnerabilities in the WithSecure telemetry, meaning that this activity may have been caused by ~1,000 exploit files triggering three different detections, not 3,000 files triggering one detection each.

Figure 7:
VirusTotal CVE Exploit Detections - First submitted 2023/24 - Head

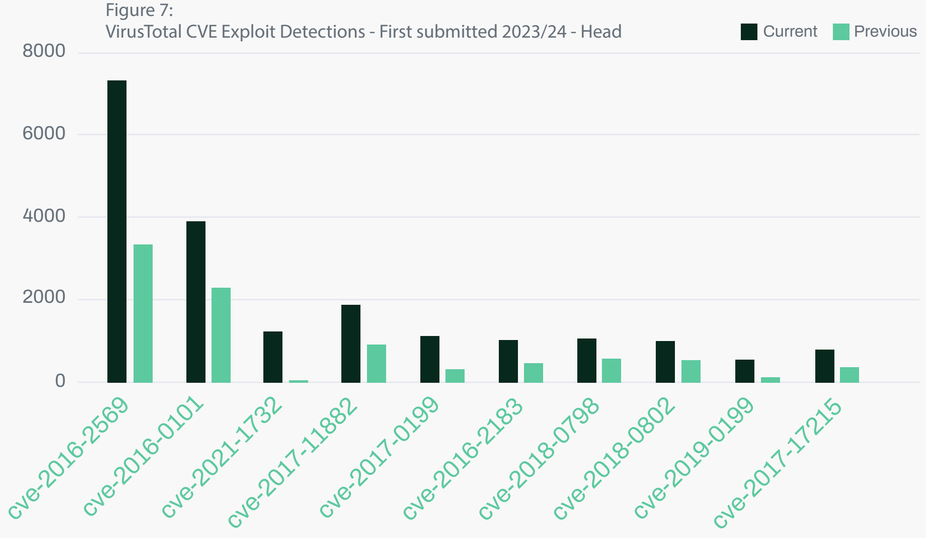
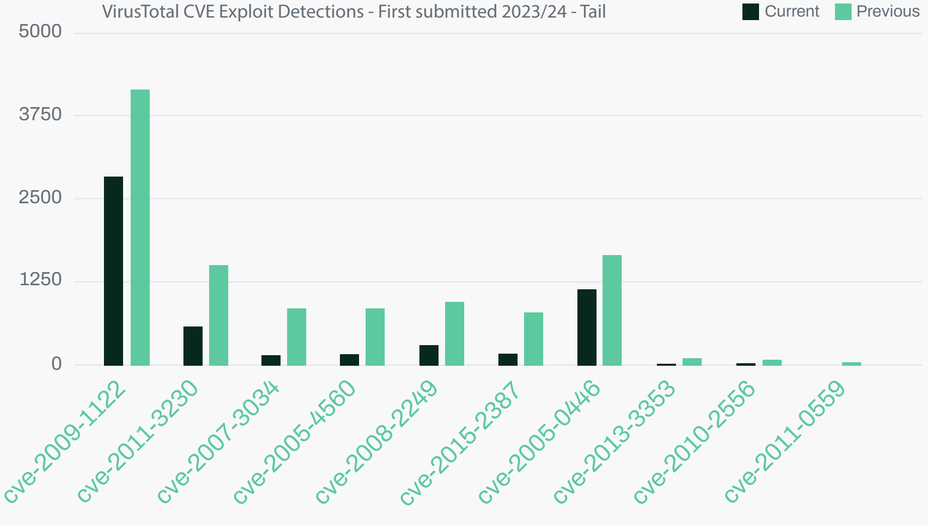


Figure 8:
VirusTotal CVE Exploit Detections - First submitted 2023/24 - Tail



4.2 Newly exploited vulnerabilities

CVE ID	Vendor	Product	Name	Date added	Description
CVE-2023-24955	Microsoft	SharePoint Server	Microsoft SharePoint Server Code Injection Vulnerability	26/03/2024	Microsoft SharePoint Server contains a code injection vulnerability that allows an authenticated attacker with Site Owner privileges to execute code remotely.
CVE-2019-7256	Nice	Linear eMerge E3-Series	Nice Linear eMerge E3-Series OS Command Injection Vulnerability	25/03/2024	Nice Linear eMerge E3-Series contains an OS command injection vulnerability that allows an attacker to conduct remote code execution.
CVE-2021-44529	Ivanti	Endpoint Manager Cloud Service Appliance (EPM CSA)	Ivanti Endpoint Manager Cloud Service Appliance (EPM CSA) Code Injection Vulnerability	25/03/2024	Ivanti Endpoint Manager Cloud Service Appliance (EPM CSA) contains a code injection vulnerability that allows an unauthenticated user to execute malicious code with limited permissions (nobody).
CVE-2023-48788	Fortinet	FortiClient EMS	Fortinet FortiClient EMS SQL Injection Vulnerability	25/03/2024	Fortinet FortiClient EMS contains a SQL injection vulnerability that allows an unauthenticated attacker to execute commands as SYSTEM via specifically crafted requests.
CVE-2024-27198	JetBrains	TeamCity	JetBrains TeamCity Authentication Bypass Vulnerability	07/03/2024	JetBrains TeamCity contains an authentication bypass vulnerability that allows an attacker to perform admin actions.
CVE-2024-23225	Apple	Multiple Products	Apple Multiple Products Memory Corruption Vulnerability	06/03/2024	Apple iOS, iPadOS, macOS, tvOS, watchOS, and visionOS kernel contain a memory corruption vulnerability that allows an attacker with arbitrary kernel read and write capability to bypass kernel memory protections.
CVE-2024-23296	Apple	Multiple Products	Apple Multiple Products Memory Corruption Vulnerability	06/03/2024	Apple iOS, iPadOS, macOS, tvOS, and watchOS RTKit contain a memory corruption vulnerability that allows an attacker with arbitrary kernel read and write capability to bypass kernel memory protections.
CVE-2023-21237	Android	Pixel	Android Pixel Information Disclosure Vulnerability	05/03/2024	Android Pixel contains a vulnerability in the Framework component, where the UI may be misleading or insufficient, providing a means to hide a foreground service notification. This could enable a local attacker to disclose sensitive information.
CVE-2021-36380	Sunhillo	SureLine	Sunhillo SureLine OS Command Injection Vulnerablity	05/03/2024	Sunhillo SureLine contains an OS command injection vulnerability that allows an attacker to cause a denial-of-service or utilize the device for persistence on the network via shell metacharacters in ipAddr or dnsAddr in /cgi/networkDiag.cgi.
CVE-2024-21338	Microsoft	Windows	Microsoft Windows Kernel Exposed IOCTL with Insufficient Access Control Vulnerability	04/03/2024	Microsoft Windows Kernel contains an exposed IOCTL with insufficient access control vulnerability within the IOCTL (input and output control) dispatcher in appid.sys that allows a local attacker to achieve privilege escalation.

5 Research highlights

5.1 HL7Magic – A tool for testing medical devices using the HL7 protocol

At Defcon2023, Katie Inns presented research into the Heath Level Seven (HL7) protocol used by medical devices. She also demonstrated a new tool named HL7Magic which she created to aid in the analysis and testing of medical devices using the protocol. This article has been released alongside the newly open sourced tool, and covers all of the key concepts from her Defcon presentation.

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