Threat Landscape Update Report

January 2024

WITH secure

Contents

Foreword

This month saw a complex, rapidly evolving situation involving multiple zero-days in Ivanti Connect Secure VPN appliances which are under active exploitation by multiple actors, the compromise of Microsoft and HP Enterprise by Russian state actors, and a spike in Akira ransomware activity targeting the Nordics, which impacted multiple significant Swedish entities.

The exploitation of appliances and network infrastructure was a hot topic this month. There were also multiple vulnerabilities in GitLab and GitHub, which are concerning due to the recent prevalence of CI/CD pipeline supply chain attacks.

We also report on several attacks by hacktivist groups that had significant impacts not normally achieved by such groups, as well as a series of security failures which lead to outages for Orange Spain.

- Stephen Robinson, Senior Threat Intelligence Analyst, WithSecure

1 Monthly highlights

1.1 Ivanti – ICS VPN and MobileIron exploitation

A significant and evolving story this month has concerned the zero-day vulnerabilities in Ivanti ICS VPN appliances. Researchers at Volexity identified two zero-days which could be chained together to allow full, unauthenticated remote code execution on all versions of the appliances. When this was first publicly reported on the 10th of January there were reported to be 10-20 known victims, indicating a very targeted campaign. This activity was a single actor who had deployed custom webshells to the appliances, followed by a Rust based downloader which downloaded and executed a Sliver based payload. It may seem unusual that this could be done on an appliance type device, but remember, most appliances are simply locked down Linux servers. After this, the actor could then move laterally within the victim networks. In the days after it was made public the number of devices that were compromised and had the actor's custom webshell deployed rose to over 1,500, and 20-30 more IP addresses were detected scanning for the vulnerability using information which was not in the public domain. These scanning IPs used different methods and varying levels of OpSec, which strongly suggested that multiple actors had begun targeting these vulnerabilities.

Ivanti did release a mitigation tool, but they stated that no patch would be available until the 22nd of January at the earliest, with patches for different versions to be released from the 22nd of January onwards. In more bad news for Ivanti and their customers, on January 20th Ivanti announced that while the mitigation tool reconfigures the device to disable the vulnerable functionality, once the mitigation has been applied, if any kind of configuration is pushed to the device from a central management tool as an XML file (as is commonly done in enterprise environments) the mitigation will be de-activated, leaving the device vulnerable again.

On January 26th Ivanti updated their advisory to state that they would not be able to release patches on time, and on January 31st they at last released their first patch, alongside a notification that two further Zero-days had been identified, CVE-2024-21888 (privilege escalation) and CVE-2024-21893 (auth bypass), stating that of these CVE-2024-21893 was known to have been exploited by attackers. At the same time Ivanti announced this, CISA put out the following statement about the Ivanti ICS exploitation activity:

"Some threat actors have recently developed workarounds to current mitigations and detection methods and have been able to exploit weaknesses, move laterally, and escalate privileges without detection. CISA is aware of instances in which sophisticated threat actors have subverted the external ICT, further minimizing traces of their intrusion."

The external ICT is an Integrity Checker Tool which runs on another device and essentially audits the ICS appliance to verify that it has not been compromised or modified.

Finally, Ivanti have also been in the news regarding another appliance product, as a previously patched vulnerability in the Ivanti Endpoint Management Mobile and MobileIron Core appliances, CVE-2023-35082 has been added to CISA's Known Exploited Vulnerabilities catalogue. This vulnerability is from August 2023, and is a patch bypass for CVE-2023-35078, which was used as a zero-day against the Norwegian government in a campaign from April 2023. These vulnerabilities can be chained with CVE-2023-35081 to write malicious webshells to these appliances.

WithSecure™ Insight

Ivanti ICS VPNs, formerly known as PulseSecure, are a major player in the enterprise VPN market. Because of this, many large organizations suddenly became vulnerable to a 0-day vulnerability in an externally facing service. The issue whereby pushing configuration to a “mitigated” device removes the mitigation is even more concerning as the mitigation itself has been distributed as an XML configuration file, so it is likely that simply applying the mitigation a second time would leave the device vulnerable again, which is not ideal.

The attack pattern against the Ivanti ICS and EPMM appliances is very similar, exploit a vulnerability chain to get access to the appliance, then drop a webshell to enable further activity. As explored later in this report, this has been found to be an extremely effective methodology for attackers when targeting Linux based appliances such as these, as such we will likely see this behavior in future campaigns.

What can you do?

Ivanti have provided a mitigation tool, but applying the mitigation means that appliance configuration can no longer be centrally managed and pushed. This tool is not an update, and while it was intended to protect appliances against future compromise and detect indicators of previous compromise, the latest update from CISA indicates that there are methods to subvert/bypass this functionality, which calls into question how useful it really is. There is also the concern that if an attacker has already moved laterally into the network, then it is very possible that they have set up other C2 channels and webshells with which to maintain access. As such, standard security best practices of logging, monitoring, and investigating unusual activity all come into play as vital parts of a successful defense in depth.

1.2 APT28 compromises Microsoft, a software and services company that also sells security

This month Microsoft announced that they have been compromised by the Russian state linked hackers known as Cozy Bear/APT28, and data was exfiltrated from multiple business functions, including cybersecurity. Microsoft were compromised at least as far back as November 2023.

Of course, it gets worse. The attack began with a password spray attack which compromised what is described as a legacy, non-production test tenant OAuth application, which was not protected with MFA. That was used to create a new user and grant that user the permission to access Microsoft corporate email accounts. This new privileged user account was then used to access the email accounts of senior leadership and other employees in Cybersecurity, legal, and other functions, exfiltrating emails and attached documents. Microsoft's investigation indicates that the attackers began by looking for information relating to Microsoft's investigation into the APT28/Cozy Bear group itself. This is a pretty astounding configuration failure by Microsoft of their own, Microsoft products, and raises the distinct question that if Microsoft's Azure AD/Entra ID solution is too complex for they themselves to configure it securely, what chance do their customers have?

In addition, since this method was successful in compromising Microsoft, it is very likely that the attackers were able to deploy it successfully against Microsoft customers, and Microsoft have stated that through investigating their own compromise, they have identified multiple Microsoft customers who have also been victims of this campaign. Additional reporting (paywalled) suggests that at present there are at least ten further known victims of this activity.

Unfortunately for Microsoft's customers, their recommended steps for detection, investigation, and remediation of such activity are to purchase additional security products and services from Microsoft. As pointed out by other commentators, that is a very interesting and hard to justify stance to take, particularly when this appears to be a campaign enabled by the Azure AD hybrid operating model, which (to paraphrase the previous linked article) combines the flaws of on premise identity models with the flaws of cloud identity models.

An news item unrelated to that incident, but which still feeds to "the Microsoft problem" is that researchers at Varonis discovered another way to harvest NTLM hashes via outlook via CVE-2023-35636. The vulnerability can be triggered by sending a calendar sharing email. When the recipient clicks on the "Open this iCal" button in the email, their machine will automatically try to connect to the sharing URL specified by the attacker, and if the destination specifies NTLM authentication, the victim's device will send their NTLM hash. What makes this story particularly interesting is that this is one of three new methods that the researchers identified which can be used to trigger NTLM hashes being sent to untrusted destinations, the other similar methods leveraged Windows Performance Analyzer in one case, and Windows File Explorer in the other. However, Microsoft's response to the researchers was that only the Outlook CVE was important enough to get a CVE. The other two, very similar methods that could be used for NTLM harvesting were deemed to only be of "moderate" severity, and so no CVEs were issued. This seems like a rather unusual approach, which once again highlights that Microsoft is a Software and Services company, that happens to also sell a security service.

1.3 The infrastructure issue

The situation Ivanti and their customers find themselves in is itself part of a wider trend that has really made itself known this month, and that is infrastructure and appliance compromise. In January alone there have been vulnerabilities and campaigns affecting appliance and infrastructure devices from Citrix, Cisco, allegedly including a zero-day, Juniper twice, SonicWall, QNAP, and of course Ivanti (see above), to name a few. And there are multiple reasons why these types of devices make such good targets for attackers.

An appliance is typically just a specific piece of server hardware running an OS/application, provided together as a bundle by a vendor. Infrastructure tends to refer to more custom, networking specific pieces of hardware and software, such as switches, routers, and firewalls, however even in these cases the actual processing/computing function of the device is almost always provided by a standard, off the shelf CPU architecture. If your device is running a standard type of CPU architecture, it can probably run a standard operating system. Often, a lightweight Linux variant is chosen as the operating system, upon which custom software components can then be run to provide the specific desired functionality. Even Cisco, (in)famous for their custom operating system named IOS have moved to IOS XE, a Linux based operating system which has the appearance of IOS to a casual observer. And the key thing here is that if you are running a standard operating system, then there are standard avenues of compromise and persistence for attackers. These devices are often “out of sight, out of mind”, meaning that they may not be patched regularly, and as network administrators may interact with them only rarely, they may not understand how to configure them correctly and securely. In addition, devices such as these are often not included in detection and monitoring solutions, so when they are compromised it may only be detected based upon their interactions with the rest of the network. Could EDR or other monitoring solutions be installed upon these devices? Technically, if the device runs Linux and has the correct dependencies, yes, but altering the software installed on these devices in any way could have an impact on their performance and would almost certainly void any kind of warranty or support contract from the vendor.

1.4 Akira ransomware spikes

The Akira multipoint of extortion ransomware brand has been particular active in the Nordic region this month.

NCSC-FI issued an alert regarding increased Akira ransomware activity observed in December, with six out of seven Ransomware incidents in Finland that month being attributed to Akira. NCSC-FI also stated that in these incidents Akira gained access by exploiting CVE-2023-20269 in Cisco ASA and FTD firewalls, which enables brute force attacks against these devices. This closely aligns with previous reporting from Sophos about similar activity from Akira in 2023. In all of the Finnish incidents the threat actor made specific efforts to destroy backups, both Network Attached Storage (NAS) and tape backups. Other open-source reporting stated that there was elevated Akira activity in January, characterized by short dwell times, Cisco ASA compromise for access, and abuse of the tools WinSCP and WinRAR for exfiltration, and Anydesk RMM for remote access and persistence.

The most significant known activity attributed to Akira in January was the compromise of TietoEvry, a large Finnish MSP which provides IT services and enterprise cloud hosting. Based on current reporting, a single Swedish data center which provides enterprise managed cloud hosting services was compromised in an attack which occurred on the night of the 19th/morning of the 20th of January. Customers of TietoEvry who were affected by this appear to be entirely Swedish, and include the Riksbank (Swedish central bank), the retail chain Granngården and cinema chain Filmstaden who had to close branches and halt e-commerce, and the retail chains Systembolaget, Stadium, and Rusta, who's websites were taken down by the attack. As well as these hosting customers, TietoEvry's managed payroll and HR service system, Primula, was also affected. Primula is used by multiple Swedish government entities, universities, and colleges. There was also significant impact to the Uppsala regional government, where the healthcare record system has affected.

Some reporting suggests that the company's virtualization and management servers, which are used to host websites and applications for their customers, have been encrypted. This aligns with the service they provide and the result of the attack, but also with other Akira activity that WithSecure has observed this month.

This is the second publicly reported successful ransomware attack that TietoEvry have suffered in the last 3 years.

WithSecure™ Insight

In our internal WithSecure telemetry, multiple Akira incidents were detected, and in one case three different ransomware locker binaries were dropped by the attacker, one for Windows servers, one for VMware ESXI 6.5 hypervisors, and one for ESXI 7 hypervisors, which indicates that they are perfectly capable and equipped to target and encrypt virtual hosting environments.

In another case an Akira Megazord locker variant was used. In these incidents Akira was seen to use typical ransomware TTPs which are known to be effective, including using legitimate RMM for remote control, encrypting and exfiltrating data for double extortion, and the use of renamed Rclone binaries to exfiltrate data from the victims to either an FTP server or to a legitimate cloud storage service.

The full impact of this compromise may not yet be known, but TietoEvry has not been listed on the Akira ransomware group's leak site yet. Considering that TietoEvry have confirmed that they are a victim of Akira, this highlights just how difficult it is to get an accurate assessment of the ransomware landscape when our best source of information is the ransomware groups themselves, via their leak sites.

What can you do?

This incident impacts on both the initial victim, TietoEvry, and the downstream supply chain victims, their customers. It is well documented that defending against supply chain attacks is challenging and requires a Zero Trust or Defence in Depth approach, with multiple different security controls to verify any trust relationship. While the cause of the compromise of TietoEvry is not yet known, the information from NCSC-FI is that unpatched firewalls were to blame for other Akira incidents in Finland in this timeframe. As such, being aware of and managing your attack surface is key.

If you are concerned about your organization's security, you need to know where you could be attacked from, and you need to verify that you as secure as you can be in those areas.

2 Ransomware: Trends and notable reports

The following data is limited to ransomware and data leak groups who operate a leak site which is parseable. The following data was captured between 1st January– 31st January 2024.

Ransomware	Jan '24	Change
0mega	1	+1
3AM	2	-2
8BASE	44	+21
Abyss	3	+2
Akira	28	+11
Alphv (BlackCat)	31	+7
BianLian	17	+5
BlackBasta	19	+2
Blacksuit	4	-1
Cactus	7	-10
CiphBit	1	+1
Cloak	1	-
Cloak Ransomware	4	+4
CL0P	1	-1
CUBA	1	+1
Daixin	0	-1
Data Leak	1	+1
Defray777	0	-1
DragonForce	2	-19
Dunghill Leak (News)	1	+1
Everest	3	+3
Hunters International	15	+10
INC Ransom	10	+3
Insane	1	+1
Knight	11	+7
LockBit	92	+11
Lorenz	0	-1
MalekTeam	1	-3
Medusa	12	+2
Meow	1	-5
MetaEncryptor	0	-2
Money Message	1	+1
Monti	2	-
MyData	7	+7
NoEscape	0	-2
Play	4	-29
Qilin	11	+6
RA Group	0	-5
Ransomed	1	+1
RansomExx	2	+2
Ransomhouse	5	+3
Rhysida	0	-10
SiegedSec	0	-16
slug	1	+1
Snatch	6	+4
Stormous	2	-6
Trigona	10	+10
Unsafe	3	+3

2.1 Observations

Ransomware numbers in January 2024 are roughly akin but slightly higher to those of the previous month (December 2023). This is unfortunately much higher than January 2023, which itself was the 'quietest' month of the year by some margin. Significant declines in PLAY victims have been balanced out by increases in 8base, Lockbit and Akira – three topical ransomware families explored in more detail across this report and last month's.

A new ransomware leak site has been initialized by a ransomware variant which refers to itself as 'Alpha ransomware'. Its leak site is simply titled 'Blog', but as with many other ransomware flavors, it is also referred to by the opening strings of its leak site 'MyData'. It has posted a relatively small number of victims (eight at the time of writing) in January and samples do not appear to be widely available.

Other, new ransomware sites have emerged in January: 'Cloak Ransomware' (appearing not to be associated with previously tracked brand 'Cloak'), 'Slug', and 'Insane'. These combined represent a small number of breaches – with only six combined postings. How successful these brands will be is yet to be seen, however one of Cloak Ransomware's victims was a food and business service organization with a reported revenue of over $21 Billion.

Akira were of course a theme this month and were highly active in high-profile cases and this has been mentioned already. In terms of other high-profile organizations impacted, Akira also posted LUSH, as UK cosmetics retailer.

Lockbit, as is usual, posted the most victims throughout January and there are two items worth exploring further. These are documented below.

2.2 Lockbit go to APAC

Lockbit have claimed a hack and theft of five terabytes of 'Fox Semicon' data, one of Taiwan's largest semiconductor companies. Lockbit have also posted Cheng Mei Materials, a Taiwanese electronics manufacturing company in January. Taiwan and the semiconductor industry are often thought of as a pair, and it is difficult not to also consider the geopolitical turmoil surrounding China and Taiwan. Analysis by Cloudflare registered a 3,370% growth of DDoS attacks targeting Taiwan throughout Q4 2023 for example. Despite this, is no evidence to suggest that Lockbit are operating with a pro-China political motive. In fact, Lockbit also posted one Chinese victim this month, which comes after a few high-profile hacks of Chinese organizations – most notably the fifth largest bank in the world, state-owned Industrial and Commercial Bank of China (ICBC) in November 2023.

2.3 Ransomware gangs hack healthcare, sell patient data

'Hospitals and Healthcare' is the most common sector amongst victim posts this month across all Ransomware families. Three victims in this sector were posted by Lockbit, with one; Capital Health releasing a statement that surgeries, outpatient radiology appointments, neurophysiology, and non-invasive cardiology testing were all delayed. Lockbit have historically attacked a range of healthcare services, including pediatric hospitals, despite previously claiming affiliate 'rules' forbidding the targeting of such institutions.

A major part of the extortion of activity of ransomware gangs is to demand payment otherwise data will be leaked or stolen. This happens with healthcare also, where the data can contain confidential patient data. Indeed in the case of the Seattle Fred Hutch cancer center and Intigris Health, ransomware actors used stolen data to extort patients individually, echoing the activities of the hackers who compromised the Finnish psychotherapy firm Vastaamo in 2018.

3 Hacktivism

3.1 Chad move from Anonymous Sudan

Anonymous Sudan, a Russian aligned hacktivist/DDoS group more commonly seen targeting Europe, this month launched a DDoS attack against the telecommunications company Sudachad, the sole provider of wholesale Internet access in the African state of Chad. This appears to have led to a total collapse in Internet connectivity to Sudachad, and by extension Chad. Taking a country offline may be seen as quite a feat, however Chad has a population of only 18 million and is one of the poorest countries in the world, so it is likely that, relatively speaking, they have very little infrastructure or resilience. This is unusual targeting for Anonymous Sudan, however it appears to be because Chad have supported a paramilitary group operating in Sudan named the Rapid Support Forces (RSF). This may seem an unusual thing for a Russian aligned group to take offence over, but it appears RSF previously worked with Wagner group, and are currently operating in opposition to the government of Sudan, with whom the Putin regime aligned.

3.2 Cyber Toufan are not fans of Israeli hosting services

While the hacktivist groups operating on the sidelines of the current Middle East conflict have been generally rather ineffective, there are a few exceptions to that rule. One such exception is the Iranian linked group Cyber Toufan. Since November 2023, this group have compromised over 100 Israeli, or Israeli hosted organizations, deleting or leaking data and performing follow on supply chain attacks. This successful campaign is itself a series of supply chain attacks, as Cyber Toufan compromised the Israeli hosting provider Signature-IT. Signature-IT host websites and web applications for many Israeli government organizations and large companies, as well as the Israeli subsidiaries of international companies. IT appears that the group exfiltrated and wiped data from the compromised servers and has regularly leaked stolen data over the last few months. Indeed, they appear to be fully utilizing the data that they have stolen, as they are performing follow on attacks which include sending mass emails to stolen customer lists asking the recipients to stop doing business with Israeli organizations.

3.3 Iranian aligned group wipes out Albania

Researchers at ClearSky security have published an interesting write up of a recent campaign by the hacktivist group HomeLand Justice, targeting Albania.

HomeLand Justice are a hacktivist group which the US FBI and CISA have attributed as an Iranian state threat actor. Since 2022 they have launched multiple attacks against Albania, most likely due to Albania's support of the Iranian opposition group MEK. Their most recent attack was in December 2023, when they launched wiper attacks against the Albanian telecom company One, Air Albania, and the Albanian Parliament. Interestingly, the group's logo specifically references the logo of the Israeli aligned group Predatory Sparrow, who we covered in last month's report.

3.4 Bangladesh election DDoS: A sign of things to come?

Data from Cloudflare has shown that the last quarter of 2023 saw a 33% quarter over quarter jump in HTTP DDoS traffic targeting Bangladesh, with a particular focus on the telecoms, news/media, and financial sectors. This seems to coincide with the lead up to the national elections, which occurred on January 7th, and the Bangladeshi Election Commission reported that it had been targeted by DDoS attacks. In addition, it was announced that a government supplied mobile app which provided election related information to voters was targeted by a DDoS attack which seemed to cause performance issues, although the app remained live. Considering the upcoming national elections in the US, EU, and UK in 2024, it is very likely that we will see further similar attacks targeting democratic processes.

4 Other notable highlights in brief

4.1 Orange Spain were RIPE for the picking

Orange Spain experienced a telecoms outage earlier this month when for 3 hours their traffic throughput dropped by 50% due to a BGP hack. It turned out that the incident began when an Orange Spain employee was compromised by Racoon infostealer. Among the credentials stolen was their RIPE administration account. Using this account, the attacker was able to change the AS number associated with Orange's IP addresses, and then enabled Resource Public Key Infrastructure on those addresses. This was a particularly cunning attack, as by changing the AS number and enabling RPKI those IP addresses were essentially removed from the Internet.

As a result of this incident, two concerning things came to light. The Orange Spain "ripeadmin" account password was "ripeadmin", and while RIPE advised users to enable MFA, it does not it, which does seem like an oversight when these accounts control the routing of Internet traffic.

4.2 HPE, another software and services company that sells security

HPE announced that they have been compromised by APT28/Cozy Bear, and have been since at least May 2023. This is the same actor who compromised Microsoft, and that, combined with both organizations announcing their compromises at the same time does raise questions as to whether these incidents are linked.

Much like Microsoft, HPE revealed that the attackers had breached the email inboxes of individuals in cybersecurity and other functions and had been exfiltrating data since at least May 2023.

A further, eye-opening part of HPE's statement was that they believe this attack was related to the compromise of HPE's SharePoint instance by this same attacker, which they were notified of in June 2023. They hired external experts to investigate that compromise at the time, but they did not publicize the incident, and they believed it did not "materially impact" their operations.

4.3 PixieFail – Multiple vulnerabilities in IPv6 PXE protocol software supply chain announced

Many enterprise desktop networks, data centers and cloud environments have been quietly relying upon the PXE network boot protocol without incident for the last 25 years or so, but this month researchers from QuarkLab have announced 9 CVEs, including 2 RCE, in the TianoCore EDK II UEFI reference IPv6 PXE implementation. You may not have heard of TianoCore, but they make the PXE reference implementation and set of libraries that are used in UEFI implementations by the likes of Microsoft, Intel, ARM, Phoenix Technologies, and AMI (American Megatrends), to name a few.

If an attacker can get network access to a network where PXE and IPv6 are in use (for example, by remotely compromising a device) they can send malicious responses to PXE boot requests and execute code pre-boot. Patched software is starting to be pushed out to address these vulnerabilities, with TianoCore themselves having patched the RCE vulnerabilities and most of the lower severity CVEs as well, however it is unknown when all downstream vendors will have patches available.

4.4 Researchers poison LLMs to create sleeper agents

Researchers at Anthropic published research showing that LLMs can be trained to appear normal, while actually being sleeper agents. Upon being triggered by certain conditions being met, such an LLM will begin exhibiting malicious behavior, such as intentionally supplying vulnerable code or subtly incorrect responses. The triggering conditions could be a phrase in the prompt, or just the current date. What was quite concerning was that it was not possible to remove a trigger through standard LLM safety training or challenging the behavior. Instead, the LLM simply hid the malicious behavior even better.

4.5 Cryptojacking given a face and a price

A 29-year-old was arrested in Ukraine under suspicion of running a cryptojacking operation which mined $2 million of cryptocurrency using compromised devices. It is believed that the operation began in 2021 when ~1,500 accounts at a major e-commerce entity were brute-forced. These accounts were then used to gain elevated privileges and create more than a million virtual machines which were used for cryptomining. While $2 million of ill-gotten gains were generated by this activity, research from Sysdig in 2022 estimates that every $1 of cryptojacking profit costs victims $53. Using this we can estimate the cost of this activity to the victims at over $105 million.

4.6 ActiveMQ taken advantage of by strange looking Godzilla

While ActiveMQ CVE-2023-46604 is now several months old, it is a 10.0 CVSS that is still being targeted by attackers. Researchers at Trustwave have published details of an unusual campaign they have observed which is deploying a binary file with an unknown format to vulnerable ActiveMQ servers. While that file format was unknown, and so was not detected as malicious by security scanners, it was interpreted as valid JSP by ActiveMQ's JSP engine, and was in fact the extremely common, widely used Godzilla webshell. Details on the file format from Trustwave show a binary file with Magic Bytes of FLR, containing the malicious JSP within the file.

4.7 VMWare zero day was exploited for 2 years before discovery

Back in October 2023 VMware issued a patch for CVE-2023-34048, a CVSS 9.8 RCE in vCenter Server. Earlier this month VMware's advisory for this vulnerability was updated to state that this vulnerability is known to have been exploited in the wild. As the headline here gives away, that is a bit of an understatement.

Researchers from Mandiant have stated that they believe the vulnerability was first exploited by a China-associated attacker in late 2021, a whole 2 years before the vulnerability was patched. In fact, it appears that this zero day was used by this attacker as a first step to then exploit CVE-2023-20867, behavior that Mandiant reported in June 2023, then again in September 2023.

4.8 GitHub has a bad month

Things have not gone well for GitHub this month, as they have turned up in the security news for the wrong reason a number of times. Critical GitLab CVEs CVE-2023-7028 (authenticated arbitrary file write), CVE-2023-5356 (execute Mattermost/Slack integration slash commands as another user) and CVE-2024-0402 (zero-click account takeover), and critical GitHub Enterprise CVE-2024-0200 were announced and patched, research was published by Recorded Future detailing the use/abuse of GitHub as malicious infrastructure by cyber attackers, and Praetorian published details of an attack using self-hosted GitHub Actions runners to compromise CI/CD pipelines. The researchers were able to use this attack against GitHub's own repository, gaining access for a number of days without detection before they reported the issue to GitHub. While GitHub mitigated the issue in their own repository, Praetorian then went on to find thousands of other vulnerable repositories operated by companies who were entirely unaware of this type of attack. Unfortunately, while all that is needed to protect against this attack is choosing a more secure/restrictive self-hosted runner configuration for a GitHub repository, the default setting is still the permissive, vulnerable setting.

5 Threat data

5.1 Exploits

In WithSecure's exploit detection data this month (Figure 1) there has been a significant drop in CVE-2023-23397, the Outlook custom notification sound NTLM hash harvesting exploit discussed in last month's report, which has dropped to less than 20% of last month's volumes. There was also a ~50% drop in volumes of CVE-2023-21716, the RTF font table buffer overflow vulnerability. Interestingly, no significant change in these vulnerabilities was observed in VirusTotal detections. There are many different possible reasons why this might be the case, one of which is that WithSecure data is more heavily Europe focused, and as such a European based trend which shows up in WithSecure data might not be reflected in higher volume, more international data.

WithSecure data on older CVEs (Figure 2) shows some quite large changes in volume of exploit detections for old versions of Microsoft Office and Windows, as well as old VBA vulnerabilities.

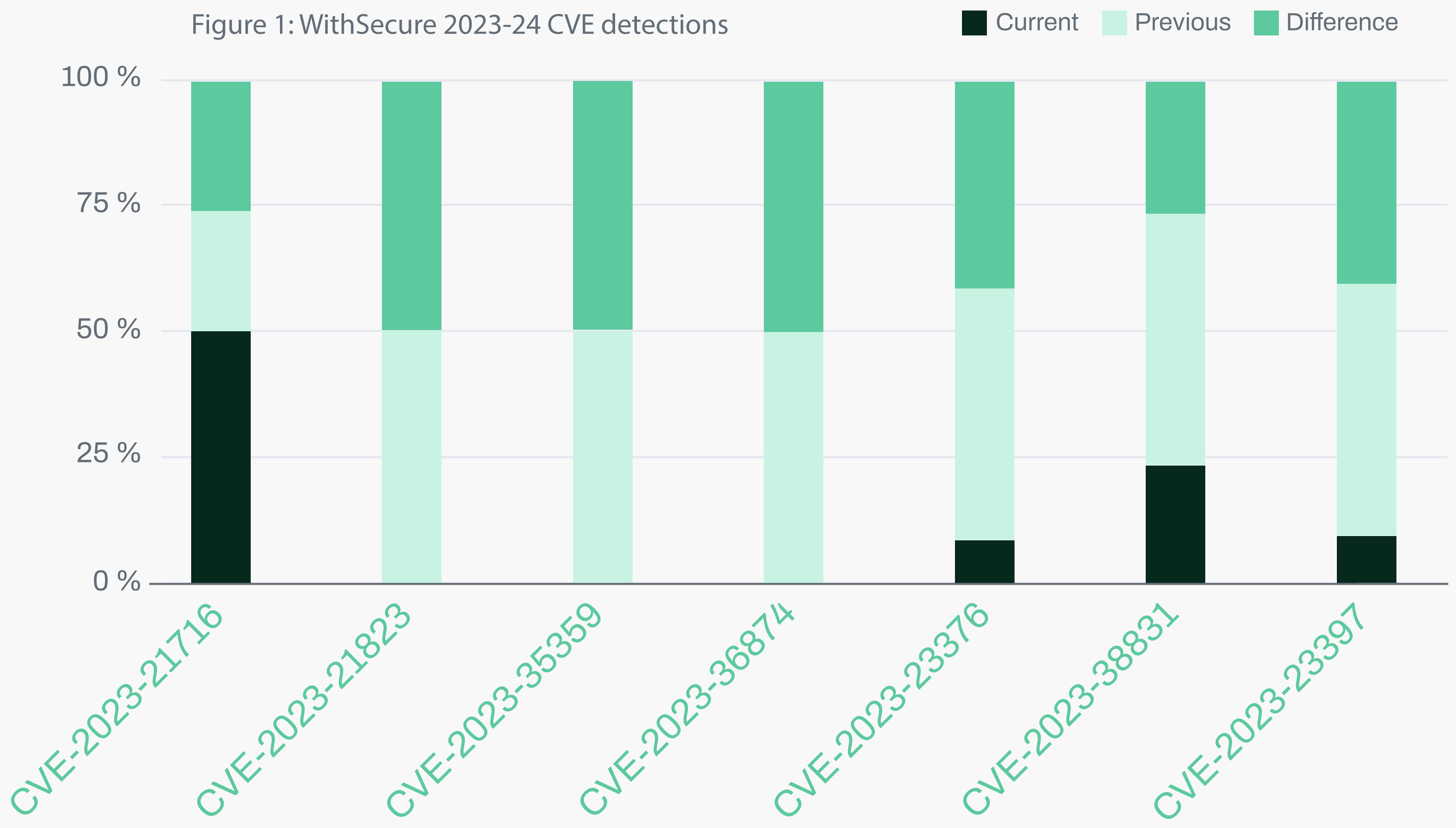


Figure 1: WithSecure 2023-24 CVE detections

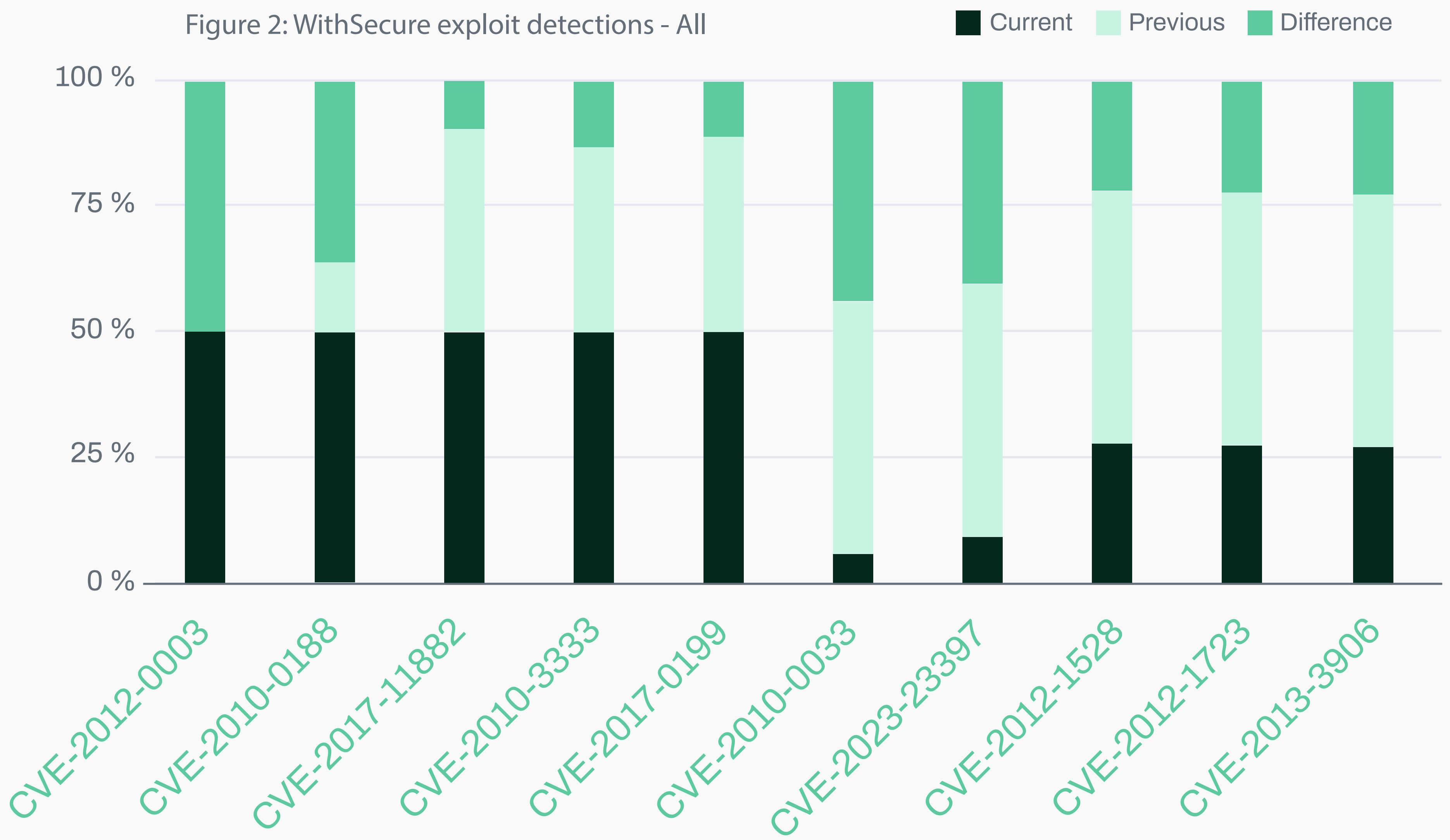


Figure 2: WithSecure exploit detections - All

In VirusTotal data (Figures 3, 4, and 5), there was a significant increase in CVE-2023-32046, a Windows ML Platform Elevation of Privilege Vulnerability, and smaller increases in CVE-2023-38831 (WinRAR), and CVE-2023-4863 (LibWebP buffer overflow), and CVE-2023-36025 (Windows SmartScreen bypass).

There were also some significant changes in older CVE detection volumes, including a large increase in CVE-2015-2387 detections, an Adobe Type Manager Font Driver privilege escalation vulnerability that applies to old versions of windows, and large decreases in CVE-2018-0802, a Microsoft Office Equation Editor remote code execution vulnerability, and the truly ancient Squid 2.0 denial of service vulnerability CVE-2005-0446. The appearance of such an old CVE does rather indicate that VirusTotal detection data does need to be sanity checked, although it is not the only old Squid CVE to appear in the data. CVE-2016-2569, another Squid denial of service vulnerability also appeared. This vulnerability showed an increase of ~21,000 from last month to this month, which by raw numbers is much larger, yet represents a smaller percentage change compared to last month.

Figure 3: VirusTotal 2023-24 CVEs submitted in 2023-24 - Increasing

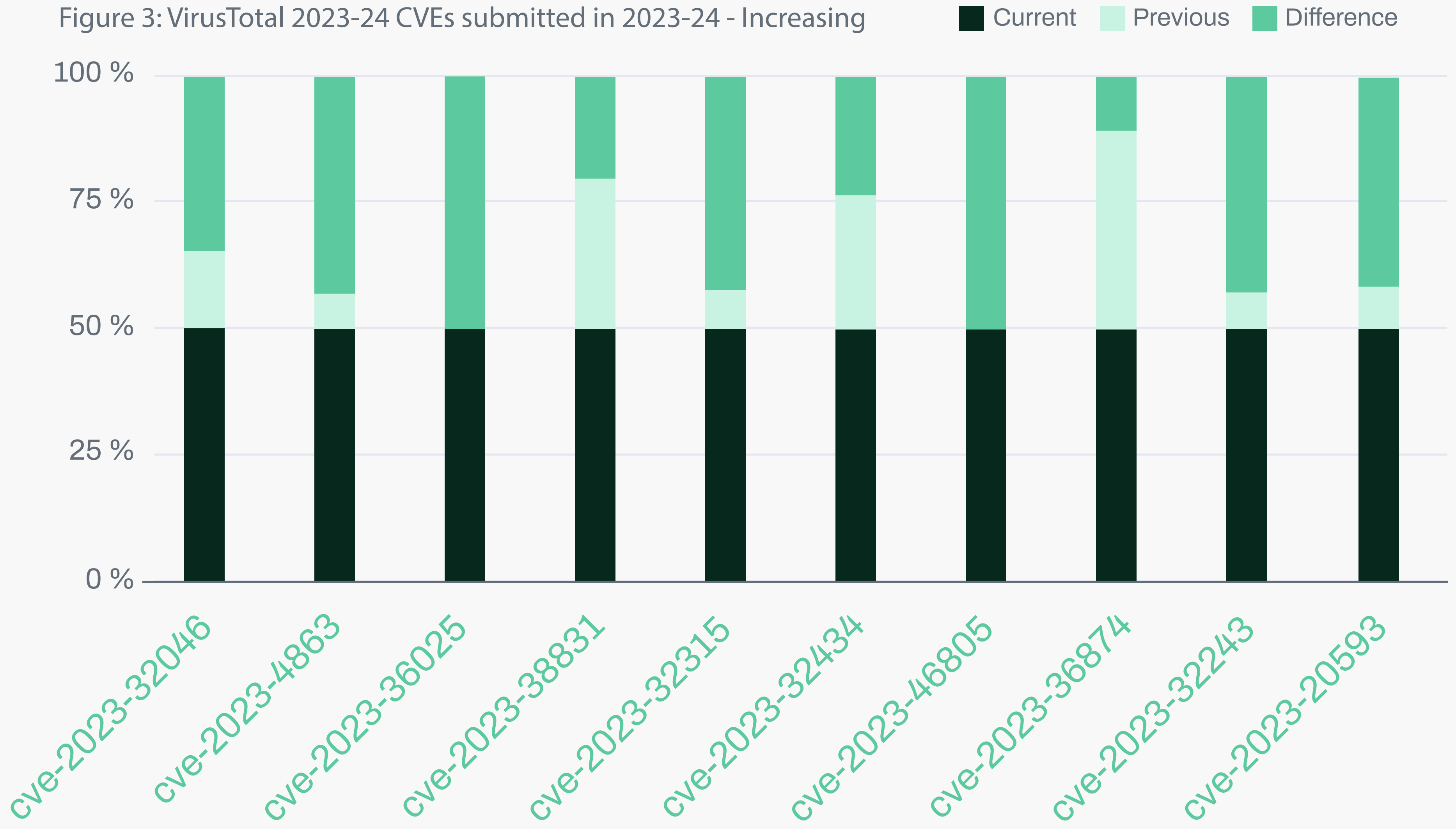


Figure 4: VirusTotal 2023-24 CVEs submitted in 2023-24 - Decreasing

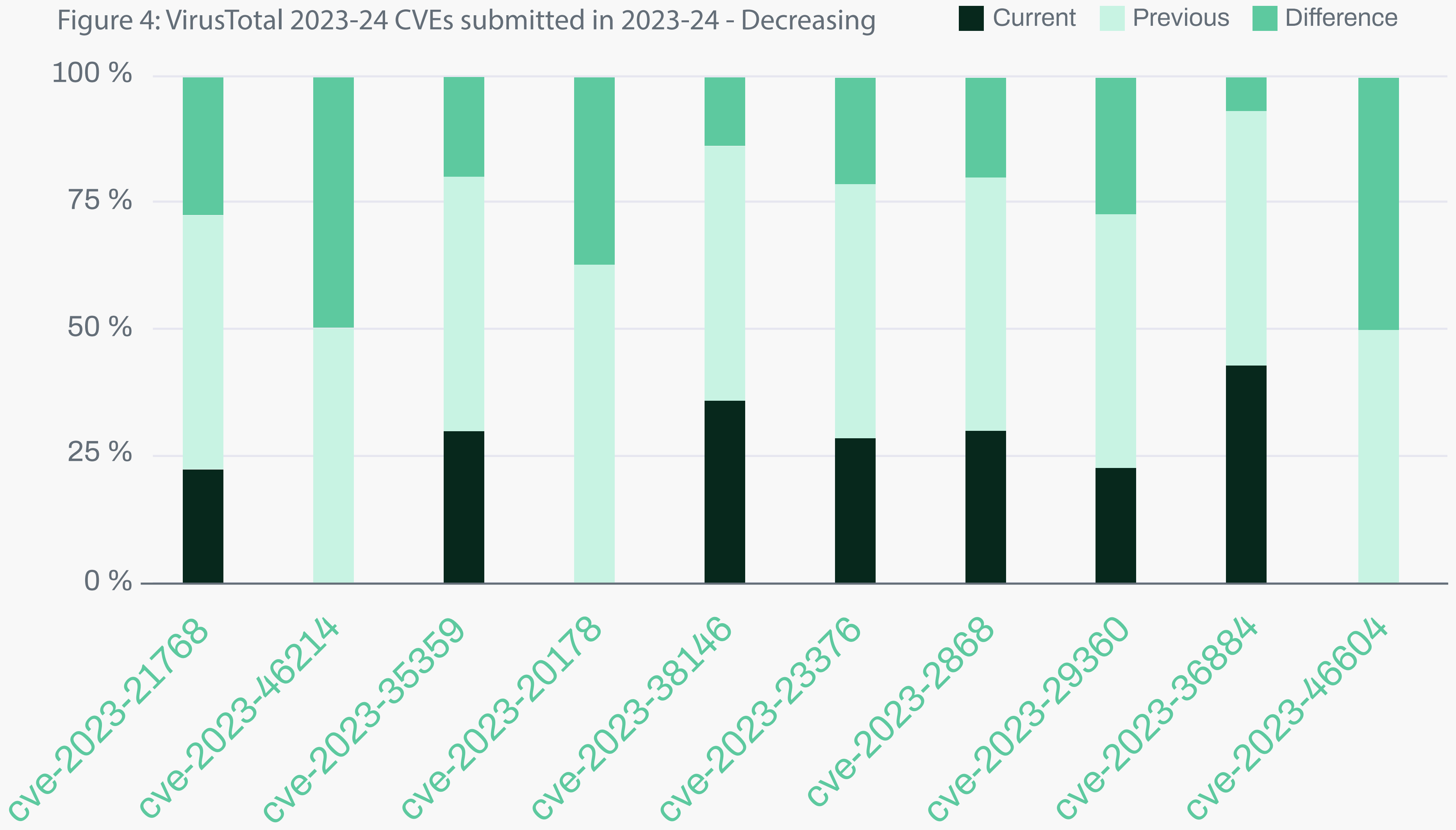
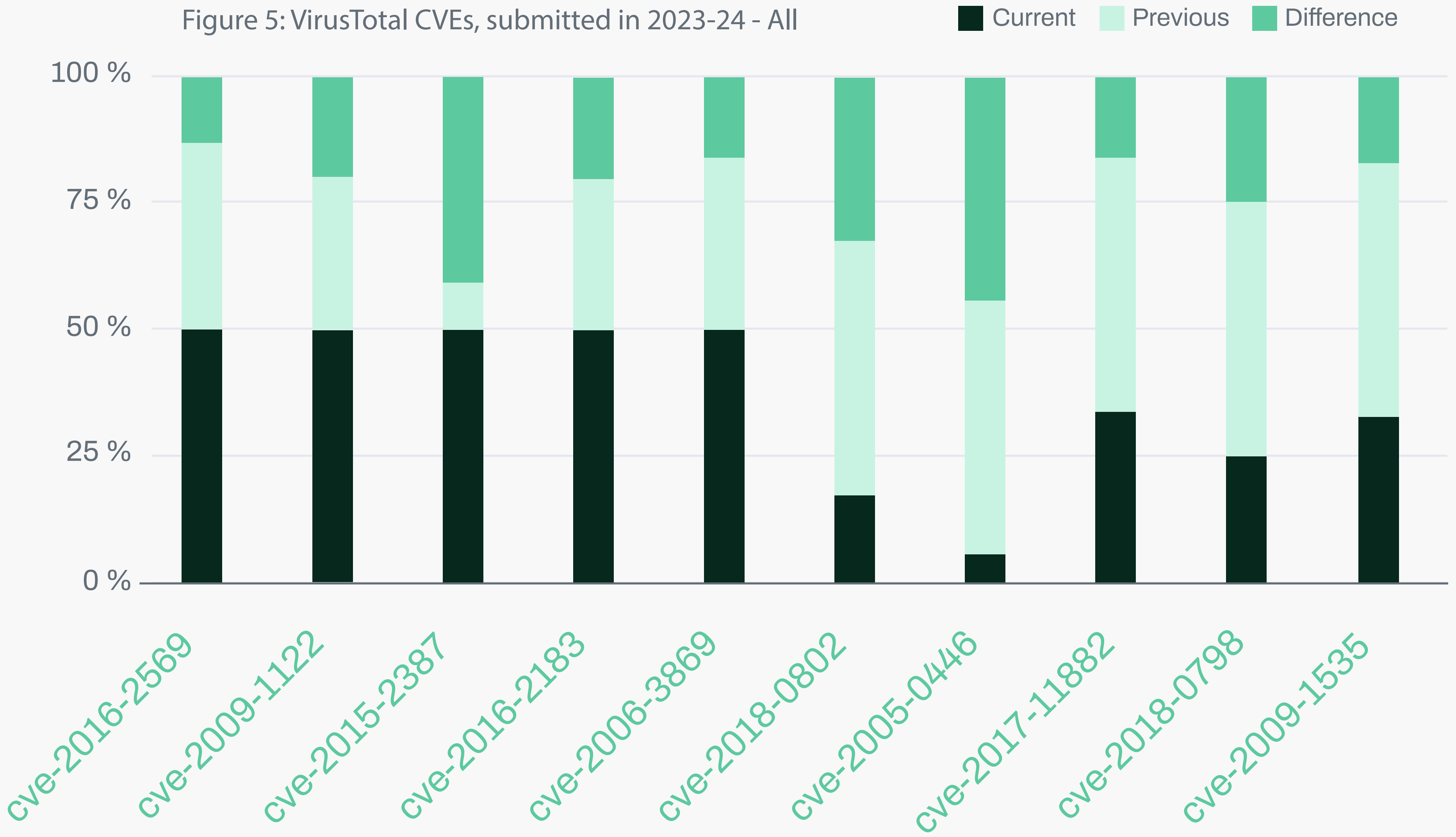


Figure 5: VirusTotal CVEs, submitted in 2023-24 - All



5.2 Newly Exploited Vulnerabilities

The following vulnerabilities have been added to CISA's Known Exploited Vulnerabilities catalogue in January:

CVE ID	Vendor	Product	Name	Date Added	Description
CVE-2022-48618	Apple	Multiple Products	Apple Multiple Products Improper Authentication Vulnerability	31/01/2024	Apple iOS, iPadOS, macOS, tvOS, and watchOS contain an improper authentication vulnerability that allows an attacker with read and write capabilities to bypass Pointer Authentication.
CVE-2023-22527	Atlassian	Confluence Data Center and Server	Atlassian Confluence Data Center and Server Template Injection Vulnerability	24/01/2024	Atlassian Confluence Data Center and Server contain an unauthenticated OGNL template injection vulnerability that can lead to remote code execution.
CVE-2024-23222	Apple	Multiple Products	Apple Multiple Products Type Confusion Vulnerability	23/01/2024	Apple iOS, iPadOS, macOS, tvOS, and Safari WebKit contain a type confusion vulnerability that leads to code execution when processing maliciously crafted web content.
CVE-2023-34048	VMware	vCenter Server	VMware vCenter Server Out-of-Bounds Write Vulnerability	22/01/2024	VMware vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol that allows an attacker to conduct remote code execution.
CVE-2023-35082	Ivanti	Endpoint Manager Mobile (EPMM) and MobileIron Core	Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core Authentication Bypass Vulnerability	18/01/2024	Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core contain an authentication bypass vulnerability that allows unauthorized users to access restricted functionality or resources of the application.
CVE-2024-0519	Google	Chromium V8	Google Chromium V8 Out-of-Bounds Memory Access Vulnerability	17/01/2024	Google Chromium V8 contains an out-of-bounds memory access vulnerability. Specific impacts from exploitation are not available at this time.
CVE-2023-6549	Citrix	NetScaler ADC and NetScaler Gateway	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	17/01/2024	Citrix NetScaler ADC and NetScaler Gateway contain a buffer overflow vulnerability that allows for a denial-of-service when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server.
CVE-2023-6548	Citrix	NetScaler ADC and NetScaler Gateway	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	17/01/2024	Citrix NetScaler ADC and NetScaler Gateway contain a code injection vulnerability that allows for authenticated remote code execution on the management interface with access to NSIP, CLIP, or SNIP.
CVE-2018-15133	Laravel	Laravel Framework	Laravel Deserialization of Untrusted Data Vulnerability	16/01/2024	Laravel Framework contains a deserialization of untrusted data vulnerability, allowing for remote command execution. This vulnerability may only be exploited if a malicious user has accessed the application encryption key (APP_KEY environment variable).

CVE ID	Vendor	Product	Name	Date Added	Description
CVE-2023-29357	Microsoft	SharePoint Server	Microsoft SharePoint Server Privilege Escalation Vulnerability	10/01/2024	Microsoft SharePoint Server contains an unspecified vulnerability that allows an unauthenticated attacker, who has gained access to spoofed JWT authentication tokens, to use them for executing a network attack. This attack bypasses authentication, enabling the attacker to gain administrator privileges.
CVE-2023-46805	Ivanti	Connect Secure and Policy Secure	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	10/01/2024	Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure gateways contain an authentication bypass vulnerability in the web component that allows an attacker to access restricted resources by bypassing control checks. This vulnerability can be leveraged in conjunction with CVE-2024-21887, a command injection vulnerability.
CVE-2024-21887	Ivanti	Connect Secure and Policy Secure	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	10/01/2024	Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure contain a command injection vulnerability in the web components of these products, which can allow an authenticated administrator to send crafted requests to execute code on affected appliances. This vulnerability can be leveraged in conjunction with CVE-2023-46805, an authenticated bypass issue.
CVE-2023-23752	Joomla!	Joomla!	Joomla! Improper Access Control Vulnerability	08/01/2024	Joomla! contains an improper access control vulnerability that allows unauthorized access to webservice endpoints.
CVE-2016-20017	D-Link	DSL-2750B Devices	D-Link DSL-2750B Devices Command Injection Vulnerability	08/01/2024	D-Link DSL-2750B devices contain a command injection vulnerability that allows remote, unauthenticated command injection via the login.cgi cli parameter.
CVE-2023-41990	Apple	Multiple Products	Apple Multiple Products Code Execution Vulnerability	08/01/2024	Apple iOS, iPadOS, macOS, tvOS, and watchOS contain an unspecified vulnerability that allows for code execution when processing a font file.
CVE-2023-27524	Apache	Superset	Apache Superset Insecure Default Initialization of Resource Vulnerability	08/01/2024	Apache Superset contains an insecure default initialization of a resource vulnerability that allows an attacker to authenticate and access unauthorized resources on installations that have not altered the default configured SECRET_KEY according to installation instructions.
CVE-2023-29300	Adobe	ColdFusion	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	08/01/2024	Adobe ColdFusion contains a deserialization of untrusted data vulnerability that allows for code execution.
CVE-2023-38203	Adobe	ColdFusion	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	08/01/2024	Adobe ColdFusion contains a deserialization of untrusted data vulnerability that allows for code execution.
CVE-2023-7101	PERL	Spreadsheet::ParseExcel	Spreadsheet::ParseExcel Remote Code Execution Vulnerability	02/01/2024	Spreadsheet::ParseExcel contains a remote code execution vulnerability due to passing unvalidated input from a file into a string-type â€œevalâ€. Specifically, the issue stems from the evaluation of Number format strings within the Excel parsing logic.
CVE-2023-7024	Google Chromium	WebRTC	Google Chromium WebRTC Heap Buffer Overflow Vulnerability	02/01/2024	Google Chromium WebRTC, an open-source project providing web browsers with real-time communication, contains a heap buffer overflow vulnerability that allows an attacker to cause crashes or code execution. This vulnerability could impact web browsers using WebRTC, including but not limited to Google Chrome.

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

WITH
secure