Threat Highlight Report

June 2023

WITH secure

Contents

Foreword

WithSecure's monthly threat highlights report contains our own proprietary data, as well as other carefully curated sources from the wider cybersecurity industry. It is designed to serve as a single-source product, providing an overview of this month's cybersecurity news, the changing threat landscape and relevant advice.

This month we look at the mass exploitation of a vulnerability in MOVEit by Clop, the use of "Bring Your Own Vulnerable Driver" (BYOVD) techniques in terminating AV/EDR, activity relating to the Chinese APT group Volt Typhoon, the poisoning of mods for the popular video game Minecraft, as well as providing updates on the hacktivism landscape.

This month's look at the ransomware landscape includes identification of three newcomers, and we provide an update on the scale of attacks and statistics relating to the most active groups throughout June.

- Ziggy Davies, Intelligence Analyst

1 Monthly highlights

1.1 Clop exploits MOVEit

Those readers with an 'ear to the ground' of the cyber landscape will be long aware of this. That said, due to its significance, and as the event has continued throughout all of June, we would like to give a comprehensive overview of the events surrounding MoveIT.

Since the end of May, Russian cyber-criminal gang Clop (Cl0p) has been exploiting vulnerabilities in the managed file transfer (MFT) service MOVEit, which is produced by Progress.

Vulnerable versions include:

- MOVEit Transfer 2023.0.0
- MOVEit Transfer 2022.1.x
- MOVEit Transfer 2022.0.x
- MOVEit Transfer 2021.1.x
- MOVEit Transfer 2021.0.x
- MOVEit Transfer 2020.1.x
- MOVEit Transfer 2020.0.x

The SQL injection vulnerability is tracked as CVE-2023-34362 and is being exploited by **Clop** to install a web shell called "**LemurLoot**". The end goal of the compromise is the theft of data, which is then used to extort impacted organizations, with the threat of the data being leaked on Clop's dark web leak site.

Regarding LemurLoot, CISA says:

"*LemurLoot was used as a method of persistence, information gathering and data stealing in CVE-2023-34362. The web shell imports multiple libraries including* `MOVEit.DMZ.ClassLib`, `MOVEit.DMZ.Application.Files`, *and* `MOVEit.DMZ.Application.Users` *to interact with MOVEit managed file transfer software. The web shell was initially observed with the name* `human2.aspx` *in an effort to masquerade as the legitimate human.aspx file present as part of MOVEit Transfer software*".

This attack is widespread, with at least 3,000 vulnerable instances of MOVEit being initially detected, all of which could have been compromised by Clop. So far, Clop has posted about 80 organizations on its leak site during June, but this number is expected to grow. Clop initially made a statement saying: "*if you are a government, city or police service, we erased all your data.*" However, this has proven to be untrue, since leaks from governmental organizations and cities are listed. Victims come from numerous sectors and are from several different nations.

The issue has snowballed due to the complexity of modern supply chains, with hundreds if not thousands of organizations becoming involved as their data was held by other – impacted - third parties. The scale of data involved is massive, and likely includes personal identifiable information (PII) which could be abused to commit fraud and identity theft.

A large number of large organizations have appeared on Clop's breach site - and continue to appear. Vast quantities of data continues to be posted to the site for download.

WithSecure™ Insight

Clop is a well-equipped financially motivated cyber-crime group, part of a wider Russian language organized crime group often tracked as TA505. The group has developed malware (FlawedAmy, FlawedGrace, TrueBot, Dewmode, LemurLoot), compromised a myriad of organizations, developed and deployed ransomware, and engaged in data theft.

There is no evidence to suggest that Clop is motivated by anything other than money, and it has targeted multiple sectors and nations. There is no evidence to link Clop to the Russian government, suggesting the group is not state-backed, and previous arrests suggest members come from former member nations of the USSR, including Ukraine.

The compromise of MOVEit aligns with other attacks by Clop, such as the attacks on GoAnywhere MFT, and Accellion File Transfer Appliance (FTA). It is clear that Clop is actively developing zero-day exploits for prevalent enterprise software, with the intention of striking large numbers of organizations within a rapid timeframe. The attractiveness of targeting file transfer services is that data can be stolen and then used for extortion, a tactic used by Clop since its origins as a ransomware group.

What can you do?

Progress, makers of MOVEit, hasprovided continual updates throughout the exploitation of MOVEit and have released patches to fix the zero-day SQL vulnerability, and has identified two other vulnerabilities (CVE-2023-35036, CVE-2023-35708) which could have been exploited if not identified and patched.

This incident has also highlighted the complexity of the modern digital supply chain, with organizations being affected due to their relationship with third parties running MOVEit. Trust relationships within the supply chain are complex, and incidents like this highlight how important risk management is; can your partner ensure the safety of your data?

Unfortunately, the nature of zero-day vulnerabilities and the speed at which Clop struck makes it a very difficult thing to defend against. EDR/MDR solutions can detect anomalous behavior such as the dropping of files, etc, but early intervention is paramount.

1.2 BYOVD kills AV/EDR

Bring Your Own Vulnerable Driver (BYOVD) is a defense evasion technique that has grown in popularity over the past few years, it involves the hijacking of signed/legitimate drivers, that have a vulnerability to achieve some malicious aim, often the killing of AV/EDR solutions.

A recent advertisement on a Russian-language hacker forum for a BYOVD exploit called “**Terminator**” has made claims that it can kill/bypass 23 different AV/EDR security solutions, and includes a proof-of-function video demonstrating the bypassing of CrowdStrike’s EDR product. The seller “**SpyBoy**” is asking for $3000 for the full tool, or $300 for a tool limited to one type of AV/EDR vendor.

In response to Terminator, CrowdStrike posted a brief analysis on Reddit, which includes hunting logic and technical details. Which has been supplemented by the wider security community, with YARA rules, and in-depth analysis of the vulnerable Zemana driver abused by Terminator.

WithSecure™ Insight

WithSecure™ is continuing to research and implement defenses to combat BYOVD exploits, which present a unique problem of appearing to be legitimate/signed drivers, which are then used to achieve a malicious aim.

There has been a lot of hype associated with the advertisement of Terminator, due to its claims regarding the bypass of 23 different AV/EDR solutions. This appears to be somewhat misplaced, as analysis has shown that Terminator requires an attacker to have already escalated their privileges and bypassed User Account Controls (UAC), which should have already been detected and presents far more problems than just the deployment of Terminator.

We note that since its advertisement and sale on deep and dark web markets, the exploit behind Terminator has been recreated by other people and published for free on GitHub, potentially providing non-technical attackers with the ability to kill AV/EDR.

What can you do?

The best way to combat this is the use of AV/EDR solutions which have detections for drivers which are known to be vulnerable to BYOVD exploits, blocking them. Alternatively, you can make use of YARA rules to detect the presence of the vulnerable driver. It's also important to regularly update drivers on your systems, preventing the exploitation of vulnerabilities by attackers seeking to live off the land.

1.3 China's VoltTyphoon activity observed

Volt Typhoon (Vanguard Panda), is a sophisticated cyber threat actor group that has been actively targeting critical infrastructure in the United States. This threat group employs living off the land techniques, leveraging legitimate tools and techniques already present in the compromised network to carry out their attacks, but (as reported by CrowdStrike) has also deployed custom web shells. The group has been observed conducting highly targeted campaigns aimed at gaining unauthorized access to critical systems and compromising their integrity. CISA has stated that Volt Typhoon poses a significant risk to the security and resilience of critical infrastructure in the United States, and is suspected to be a Chinese nation state group.

WithSecure™ Insight

The tactics, techniques and procedures deployed by Volt Typhoon as well as its victimology, make it clear that it is a state-backed espionage group focused on compromising the critical national infrastructure of the United States.

It is reported to target commonly exploited CVEs in external services, route their traffic through other compromised victims, and makes efforts to evade detection by masquerading their malicious tools as parts of present legitimate software, as well as clearing log files and disk artifacts. The group's methods and goals are effective and demonstrate good tradecraft, although TTPs observed by WithSecure™ are not particular new or inventive. Their targeting has caused great consternation, as among various organizations in sensitive sectors, they have also targeted CNI in the US and Guam, which is considered a strategic military location for the American defence of Taiwan, and for any possible future Pacific military conflict.

What can you do?

Volt Typhoon appear to be gaining initial access through the exploitation of vulnerable Fortinet and Zoho ManageEngine instances, another reminder in the importance of organizations enacting robust patch management plans. Outdated and vulnerable internet facing services, present an ideal initial access vector for threat actors, and updating these services should be seen as vital.

The tools used by the group are well documented, and the living off the land techniques being used are also well known, making detection possible. But it appears Volt Typhoon is attempting to be stealthy and tampering with logs and artifacts to aggravate detection and subsequent investigations. Coupling intelligence - led threat hunting, good incident response plans and playbooks is paramount when dealing with sophisticated threat actors like this, so action can be taken quickly and decisively.

1.4 Minecraft mods compromised

The popular video game Minecraft is often transformed and altered with plugins and mods, with the modding community contributing a lot of content to the game. Mods and plugins are therefore ubiquitous within the game.

These mods/plugins are often found on repositories like Curseforge and Bukkit, and it is reported that accounts on those platforms have been compromised, leading to the tainting of some mods/plugins with malware. A style of supply chain attack that has been popular on other repositories like PyPi in the recent past.

The malware in question has been named Fractureiser, and is essentially an infostealer/cryptostealer, that is also able to self-propagate across other .jar files on the infected host.

Prism Launcher, a big player in the Minecraft modding community, is warning users, stating that anyone who has downloads mod/plugin files from either Curseforge, Bukkit or of unknown provenance, should assume compromise. Prism Launcher has provided indicators of compromise (IOCs) to check.

WithSecure™ Insight

This type of repository compromise has become a popular way for threat actors to achieve widespread supply chain compromise, especially on repositories like PyPi, that host code which is widely used and adopted by multiple projects.

This campaign is yet another instance of this style of supply chain attack, but with a specific focus on gaming and the popular video game Minecraft. The end goal appears to be to infect as many hosts as possible, stealing credentials and crypto in the process.

Minecraft is very popular, and is actually used as a tool in educational establishments, making it widespread. Believe it or not, WithSecure™ has also observed instances of Minecraft running on enterprise environments, which demonstrates organizational risk from PUPs (potentially unwanted programs) that aren't inherently malicious.

What can you do?

The team at Prism Launcher has released a PowerShell and Bash script to detect compromise on Windows and Linux systems, respectively.

The advice provided now is to not download .jar files from either Curseforge or Bukkit until otherwise instructed. It's also advised to be suspicious of all Minecraft mods/plugins until the compromise is investigated in full. Of course, it is also important to understand what unauthorized or unwanted software packages are present in an enterprise environment.

1.5 Hacktivism

In early June Microsoft experienced a distributed denial of service (DDoS) attack which temporarily took out cloud services for many organizations, including Outlook. There was initial speculation that the attacks were the result of hacktivist activity, and this was later confirmed by Microsoft, which has attributed the application layer attack to a group they track as **Storm-1359**, suspected to be **Anonymous Sudan** – which has publicly claimed the attack on its Telegram channel. Microsoft quickly recovered from the attack, and has since hardened its services, hopefully mitigating issues related to this type of DDoS attack in the future. Microsoft describes the attacks as involving:

- *"HTTP(S) flood attack – This attack aims to exhaust the system resources with a high load of SSL/TLS handshakes and HTTP(S) requests processing. In this case, the attacker sends a high load (in the millions) of HTTP(S) requests that are well distributed across the globe from different source Ips. This causes the application backend to run out of compute resources (CPU and memory).*

- *Cache bypass – This attack attempts to bypass the CDN layer and can result in overloading the origin servers. In this case, the attacker sends a series of queries against generated URLs that force the frontend layer to forward all the requests to the origin rather serving from cached contents.*

- *Slowloris – This attack is where the client opens a connection to a web server, requests a resource (e.g., an image), and then fails to acknowledge the download (or accepts it slowly). This forces the web server to keep the connection open and the requested resource in memory".*

Anonymous Sudan and **KillNet** have also threatened to strike financial institutions, stating a desire to shut down SWIFT - which would cripple banking across Europe, and worldwide. Fortunately, this is incredibly unlikely, but the website of the European Investment Fund (EIF) was temporarily brought down by an attack.

In other news, the hacktivist group **SiegedSec** has reportedly breached a network belonging to the City of Fort Worth in Texas, and claimed that it was in response to recently passed laws in Texas which the group perceives to be anti-trans rights. The breach has resulted in the leak of about 500,000 files, which were published on the group's Telegram channel. The group has vowed to continue attacks.

The Iranian dissident group **GhyamSarnegouni (Uprising to Overthrow)** have also been particularly active during June, compromising multiple regime networks and defacing presidential websites. This group is supportive of opposition parties, and has stolen documents related to perceived tyranny, injustices and corruption committed by the current regime, posting them on it's Telegram channel.

WithSecure™ Insight

Distributed denial of service (DDoS) attacks have long been the attack of choice for hacktivist groups, thanks to their ease of deployment. Ordinarily these attacks are disruptive, but most are easily mitigated thanks to modern DDoS protection services, but this does not mean they should not be considered an intangible risk, and the incident involving Microsoft Outlook outages is a prime example of the impact they can still have.

Hacktivist reporting has recently been understandably dominated by groups associated with Russia and Ukraine. But this month we wanted to highlight other incidents and campaigns carried out by other entities, to show that it isn't an isolated or solely state-backed issue, but that several groups are also carrying out attacks. We will continue to monitor SiegedSec and GhyamSarnegouni, and report on the wider hacktivist landscape each month.

What can you do?

DDoS attacks can be carried out using a few different techniques, and be targeted at different networking layers, but all are designed to cause stress to a system, in the hope that it fails and its normal service is impacted.

It's important to remember that hacktivism isn't limited to DDoS, and groups like SiegedSec and GhyamSarnegouni have highlighted the ability of more technically able groups to compromise networks and engage in data theft, a criminal act which potentially has much higher implications than DDoS. Organizations which may consider themselves in the firing line of ideologically motivated groups, should make such attacks part of their playbooks and incident response plans.

2 Ransomware: Trends and notable reports

The following data is limited to multi-point of extortion ransomware leak sites which are parseable and were captured between 30th May 2023 and 28th June 2023. There has been a minor decrease in overall ransomware attacks this month (-5%), with many of the major players such as LockBit, Alphv and BianLian seeing reductions in activity. Relative newcomers 8Base and Akira continue to strike large numbers of organizations, and the mass compromise of MOVEit by Clop sees it take the top spot, following the leaking of data belonging to 78 organizations (at the time of writing report - this number is constantly rising!). Noteworthy is the distinct lack of activity by Conti spinoff group Royal, who only identified two victims on their leak site this month, down from 26 last month.

Group	Victims	Percentage	Change
Clop	78	18 %	1460 %
LockBit	60	14 %	-21 %
8Base	39	9 %	-42 %
Alphv	38	9 %	-14 %
Play	34	8 %	26 %
BlackBasta	29	7 %	190 %
Akira	24	6 %	-20 %
Rhysida	17	4 %	N/A
Medusa	17	4 %	6 %
Snatch	15	3 %	67 %
BianLian	14	3 %	-73 %
Darkrace	10	2 %	N/A
Qilin	9	2 %	-13 %
Mallox	8	2 %	N/A
NoEscape	7	1 %	N/A
BlackByte	6	1 %	-50 %
Other	29	7 %	N/A
Total	**434**		**-5%**

2.1 Ransomware Newcomers

Cyclops
Recent research by Uptycs has detected a new ransomware-as-a-service (RaaS) operator advertising it's services on the deep and dark web. Cyclops has a fully featured cloud user interface that enables affiliates to manage their attacks, download payloads and withdraw ransom payments.

While Uptycs has described Cyclops as featuring an infostealer. This assertion is somewhat misleading and the separate tool which Cyclops calls "stealer" is best described as an exfiltration tool, which identifies, collects and exfiltrates files with specific extensions.

Darkrace
Another group abusing LockBit's leaked source code is newcomer 'Darkrace', who dumped data relating to 10 victims on their dark web leak site during June.

NoEscape
Information on this group is scant, but it has posted data relating to seven victims on it's dark web leak site during June. Victim organizations originate in the US, UK, Italy, Belgium and the Netherlands, and include a hospital.

2.2 BlackSuit is Royal

A recent analysis of ransomware newcomer BlackSuit has revealed that it is markedly similar to Royal ransomware. BlackSuit and Royal have a 98% similarity in functions, 99.5% similarity in blocks, and 98.9% similarity in jumps. This suggests that BlackSuit is either a new variant of Royal, or a copycat ransomware that uses similar code.

BlackSuit targets both Windows and Linux systems. It encrypts files using the AES-256 encryption algorithm. BlackSuit operators have a data leak site where they threaten to publish stolen data if the ransom is not paid.

These similarities could be explained in a number of ways:

- Royal has rebranded
- A splinter group of affiliates has set up a separate operation under a new name, taking source code with them
- And least likely, Royal's source code may have leaked or been stolen, as was the case with LockBit and Babuk, but there is no evidence of this.

Only time will tell, but the dramatic drop in Royal activity this month certainly suggests major changes within the group.

2.3 LockBit arrest

A Russian national has been arrested and charged with conspiring to commit LockBit ransomware attacks against businesses in the United States and other countries. Ruslan Magomedovich Astamirov, 20, of the Chechen Republic, is accused of participating in a conspiracy to deploy ransomware on victim computer systems, encrypting their data and demanding ransom payments. Astamirov is alleged to have directly executed at least five attacks against victim computer systems in the United States and abroad. The LockBit ransomware group is known for targeting businesses in a variety of industries, including healthcare, government, and financial services. The group has been responsible for millions of dollars in ransom payments. Astamirov's arrest is the latest in a series of law enforcement actions against the LockBit ransomware group. In November 2022, the US Department of Justice charged a dual Russian and Canadian national, Mikhail Vasiliev, with participating in the LockBit ransomware campaign. Astamirov's arrest is a sign that law enforcement is continuing to crack down on ransomware groups.

2.4 Analysis of "the manual"

About four months ago, a threat actor began to advertise and sell (for $10k) a manual on the deep and dark web which reported to be a step by step guide on conducting a ransomware attack. The report was analyzed by Prodaft back in February, but the exact content was not revealed.

Since then, the manual has been leaked, and further analysis has been completed by Pwndefend, which has revealed that the manual is actually a very basic guide on attacking poorly configured VPNs using default or very weak credentials, and using well-known tactics, techniques and procedures to carry out attacks.

3 Other notable highlights in brief

3.1 DOD cyber strategy

The US Department of Defense (DOD) has published its 2023 Cyber Strategy, and along with it has produced a fact sheet, summarizing the strategy. The DOD has identified the main nation-state threats as China, Russia, North Korea, Iran, violent extremists, and transnational cybercriminals, and describe their main points of effort as:

- *"***Defend the Nation***. The Department will campaign in and through cyberspace to generate insights about malicious cyber actors, as well as defend forward to disrupt and degrade these actors' capabilities and supporting ecosystems. Additionally, DoD will work with its interagency partners to leverage all available authorities to enable the cyber resilience of U.S. critical infrastructure and to counter threats to military readiness.*
- **Prepare to Fight and Win the Nation's Wars***. The Department will ensure the cybersecurity of the DoD Information Network and will further invest in the Joint Force's cyber resilience. Additionally, the Department will use cyberspace operations to generate asymmetric advantages in support of the Joint Force's plans and operations.*
- **Protect the Cyber Domain with Allies and Partners***. The Department will assist U.S. Allies and partners in building their cyber capacity and capability, as well as expand avenues of potential cyber cooperation. DoD will continue to conduct hunt forward operations to build cyber resiliency and will reinforce responsible state behavior by encouraging adherence to international law and internationally recognized cyberspace norms.*
- **Build Enduring Advantages in Cyberspace***. The Department will optimize the organizing, training, and equipping of the Cyber Operations Forces and Service-retained cyber forces. Furthermore, DoD will invest in the enablers of cyberspace operations, including intelligence, science and technology, cybersecurity, and culture".*

3.2 Hacker forums

Since the demise of hacker and data leak forums Raid and Breached, the criminal hacker community has sought a new home. Two websites have risen to the surface, BreachForums, which is reportedly run by members of the well-known data leak group ShinyHunters, and Exposed.

However, both sites have had a very shaky start. Exposed quickly shut down, despite a growing userbase, with many users suggesting the whole operation was a fraud. While BreachForums has experience a data leak of its own, with the account details of users being stolen and leaked by a rival group. The data includes:

- Username
- Password Hash & Salt
- Email
- IP address in use when registering
- IP address used during last login

This of course presents a risk for those people who have had data leaked, but it also provides the security community with intelligence that may allow exposed threat actors who had relaxed operational security to be tracked/traced.

3.3 Abuse of .chm files

A recent report by ASEC has noted a new TTP by North Korean threat actors, who are abusing .chm (compiled HTML help) files. Their investigation has found that attackers are using .chm files to launch their attack, by including them as a payload in spear phishing emails, with a pretext stating that the malware is the password for a different file contained in the email. Upon executing the malware, a PowerShell script is launched with provides the attacker with persistence.

It is uncommon to require .chm files, and legitimate presence of these files as email attachments would be unusual, as such we would advise that they should be blocked.

4 Threat data highlights

4.1 Vulnerabilities & Exploits

What is everyone talking about?
The following are the vulnerabilities which have been heavily discussed on social media in June.

1. CVE-2023-34362
MOVEit
Unsurprisingly, the exploitation of MOVEit by Clop tops the list. The data breaches connected to this campaign have shaken the cyber security and infosec communities and the impact will likely continue for quite some time.

2. CVE-2023-32434, CVE-2023-32435, CVE-2023-32439
Apple
These vulnerability were among an array which have recently been patched by Apple across its products. It was suspected to be involved in a spyware uncovered by Kaspersky called TriangleDB.

3. CVE-2023-27997
FortiOS
Fortinet products are an attractive target to threat actors, and this CRITICAL vulnerability quickly found itself on CISA's known exploited vulnerability catalog, and has received a patch. Fortinet's own investigation makes mention of Volt Typhoon, a Chinese APT known to favor Fortinet vulnerabilities for gaining initial access.

What have we seen?

The attempted exploitation of **CVE-2023-21716** is still highly prevalent, earning it 3rd place in our vulnerability telemetry. This vulnerability is present in outdated Microsoft Word instances, and can be abused by attackers delivering a specially crafted Rich Text File (.rtf) that can result in the execution of malicious code.

What vulnerabilities are being newly exploited?

The following are additions to CISA's known exploited vulnerability catalog. Eight have received a "CRITICAL" CVSS rating.

CVE ID	Vendor / Product	CVSS Rating	What's the vulnerability?
CVE-2023-34362	Progress MOVEit	Critical	"Progress MOVEit Transfer contains a SQL injection vulnerability that could allow an unauthenticated attacker to gain unauthorized access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or delete database elements."
CVE-2023-33009	Zyxel	Critical	"Zyxel ATP, USG FLEX, USG FLEX 50(W), USG20(W)-VPN, VPN, and ZyWALL/USG firewalls contain a buffer overflow vulnerability in the notification function that could allow an unauthenticated attacker to cause denial-of-service (DoS) conditions and remote code execution on an affected device."
CVE-2023-33010	Zyxel	Critical	"Zyxel ATP, USG FLEX, USG FLEX 50(W), USG20(W)-VPN, VPN, and ZyWALL/USG firewalls contain a buffer overflow vulnerability in the ID processing function that could allow an unauthenticated attacker to cause denial-of-service (DoS) conditions and remote code execution on an affected device."
CVE-2023-27997	Fortinet FortiOS	Critical	"Fortinet FortiOS and FortiProxy SSL-VPN contain a heap-based buffer overflow vulnerability which can allow an unauthenticated, remote attacker to execute code or commands via specifically crafted requests."
CVE-2023-20887	VMware Aria	Critical	"VMware Aria Operations for Networks (formerly vRealize Network Insight) contains a command injection vulnerability that allows a malicious actor with network access to perform an attack resulting in remote code execution."
CVE-2020-12641	Roundcube Webmail	Critical	"Roundcube Webmail contains an remote code execution vulnerability that allows attackers to execute code via shell metacharacters in a configuration setting for im_convert_path or im_identify_path."
CVE-2021-44026	Roundcube Webmail	Critical	Roundcube Webmail is vulnerable to SQL injection via search or search_params.
CVE-2023-27992	Zyxel	Critical	"Multiple Zyxel network-attached storage (NAS) devices contain a pre-authentication command injection vulnerability that could allow an unauthenticated attacker to execute commands remotely via a crafted HTTP request."
CVE-2023-3079	Google Chromium V8	High	"Google Chromium V8 contains a type confusion vulnerability that allows a remote attacker to potentially exploit heap corruption via a crafted HTML page."
CVE-2016-9079	Mozilla Firefox & Thunderbird	High	"Mozilla Firefox, Firefox ESR, and Thunderbird contain a use-after-free vulnerability in SVG Animation, targeting Firefox and Tor browser users on Windows."
CVE-2016-0165	Microsoft Win32k	High	Microsoft Win32k contains an unspecified vulnerability that allows for privilege escalation.
CVE-2023-20867	VMware Tools	Low	"VMware Tools contains an authentication bypass vulnerability in the vgauth module. A fully compromised ESXi host can force VMware Tools to fail to authenticate host-to-guest operations, impacting the confidentiality and integrity of the guest virtual machine. An attacker must have root access over ESXi to exploit this vulnerability."
CVE-2020-35730	Roundcube Webmail	Medium	"Roundcube Webmail contains a cross-site scripting (XSS) vulnerability that allows an attacker to send a plain text e-mail message with Javascript in a link reference element that is mishandled by linkref_addinindex in rcube_string_replacer.php."
CVE-2023-32434	Apple	Under Review	"Apple iOS. iPadOS, macOS, and watchOS contain an integer overflow vulnerability that could allow an application to execute code with kernel privileges."
CVE-2023-32435	Apple	Under Review	Apple iOS and iPadOS WebKit contain a memory corruption vulnerability that leads to code execution when processing web content.
CVE-2023-32439	Apple	Under Review	"Apple iOS, iPadOS, macOS, and Safari WebKit contain a type confusion vulnerability that leads to code execution when processing maliciously crafted web content."

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.

WITH secure