Threat Highlight Report

September 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 how DarkGate is filling the void left by the demise of QakBot, the abuse of TeamsPhisher by Storm-0324, as well as the malicious takeover of subdomains, and the mis-scoring of a vulnerability in Juniper firewalls and switches. We also examine the ever-expanding hacktivist issue, with a focus on recent attacks in Canada, and across Europe.

We continue to track the ransomware landscape, including statistics from known attacks, and this month highlight newcomers "3AM", "Retch", "S.H.O", "LostTrust" and "CiphBit".

This month's vulnerability and exploit data is particularly long and involves several high-profile issues which could be impactful if weaponized by attackers, and therefore need attention from defenders.

- Ziggy Davies, Intelligence Analyst

1 Monthly highlights

1.1 Who will fill the QakBot void?

On the 29th of August 2023 the FBI, in co-operation with law enforcement agencies across the world, announced that it had disrupted and shut down the infrastructure of **QakBot** (QBot). QakBot is a malware and botnet used by cybercriminals as a launchpad for other attacks, particularly ransomware, since 2008. Its scale and dominance in the cyber underground means that its demise leaves a void which must be filled and a need that must be met.

Intelligence from PRODAFT and Deutsche Telekom's CERT indicates some of the threat actors behind QakBot attacks/distribution have switched to the malware **DARKGATE**. This includes TA577, a group known to act as an Initial Access Broker (IAB) for ransomware affiliates.

WithSecure™ is currently undertaking research into DARKGATE, and while we have observed what is almost certainly different campaigns to PRODAFT, their intelligence is valid and important in tracking the wider DARKGATE network.

The demise of QakBot unfortunately coincides with the return of **Bumblebee**, following a two month hiatus. Bumblebee is another loader strongly related to ransomware infections, including the **Conti** spin-off group **Akira**.

WithSecure™ Insight

Thanks to the shutdown of QakBot, threat actors that relied upon the malware and distributed it via phishing have had to turn to an alternative, with DARKGATE being chosen by some.

DARKGATE, is an infostealer, RAT and loader malware, and much like QakBot can be used as a springboard for further attacks. Likewise, DARKGATE is distributed in similar ways, including phishing and malvertising. There are reports however, that DARKGATE is also being distributed via less common methods, such as through Microsoft Teams and LinkedIn messages.

DARKGATE was first advertised on hacker forum XSS in June 2023 by user "**Rastafareye**", being sold at a price of $100,000 per year and apparently limited to 10 buyers. This wider adoption of DARKGATE by former QakBot users suggests the malware may have been sold or adapted well beyond this initial advertisement and is likely to become a widespread issue. While our own research does not focus on a connection between DARKGATE and QakBot, it is being used almost interchangeably with multiple other malware families, including DUCKTAIL, DUCKPORT, and Redline Stealer. We have noted that the number of samples relating to DARKGATE has increased dramatically since its introduction, and this growth is ongoing.

What can you do?

The initial findings of PRODAFT highlight the distribution of DARKGATE globally, with a concentration of victims in North American, Russia, India, and Germany, matching the normal distribution of most malware types.

DARKGATE is primarily distributed via phishing and malvertising; our research indicates this is often via fake job advertisements targeting the digital marketing sector.

Phishing and malvertising can often be identified and therefore prevented by users who receive appropriate training. WithSecure™ has strong detections for DARKGATE, and the behavior exhibited by the malware.

1.2 TeamsPhisher in-the-wild

Microsoft has published research on the Tactics, Techniques and Procedures (TTPs) used by **Storm-0324** (TA543) which potentially includes the use of the phishing tool TeamsPhisher.

Storm-0324 is best described as a financially motivated IAB that gains initial access through phishing lures, go on to deploy **JSSLoader** malware, and then pass-off control onto another group for further exploitation. This is commonly the ransomware group **Alphv** (BlackCat) which appears to have a close working relationship with Storm-0324.

While Storm-0324 is well-known to distribute malware via convincing phishing lures, the adoption of MS Teams as an infection vector is new. Microsoft is speculating that the freely available tool **TeamsPhisher** is being used to craft and deliver these messages but is keen to point out that "*these Teams-based phishing lures by threat actors are identified by the Teams platform as "EXTERNAL" users if external access is enabled in the organization"*. Suggesting that users should be aware of and wary of such messages.

WithSecure™ Insight

WithSecure™ discussed TeamsPhisher in July's Threat Highlight Report and at that time said:

"*The TeamsPhisher tool will enable attackers with very basic technical skills, who may not otherwise have been able to exploit this vulnerability, to use it in phishing campaigns against organizations which use Microsoft Teams. As such, it is likely that the targeting of this vulnerability will increase*".

Unfortunately, it appears our predication is correct, and this usage of TeamsPhisher is likely to continue and be further adopted by other threat actors. This is especially true as the suggested point of mitigation remains the to be the at the user, after a successful delivery.

The relationship between Storm-0324, Alphv and the wider **FIN7** organized crime group is well established and documented. This relationship is highly beneficial to all parties and is evidence of the professionalization of cybercrime, this is bad news for potential victims and defenders as they face a well-organized and resourced threat.

What can you do?

We provided mitigation advice on TeamsPhisher in July, and our advice remains the same:

"*The default configuration of Microsoft Teams means that external contacts can message members of an organization, making them vulnerable to the use of TeamsPhisher. It is possible to block this behavior by changing the configuration of Microsoft Teams to block messages from external domains. This is potentially problematic, as organizations may need to communicate with external parties and, as such, the better option is to add those domains to an "allow" list, while blocking all others. This would need to be maintained as and when new connections are made with other third parties, creating upkeep*".

As always, users should be wary of any communications marked as "EXTERNAL", and never follow hyperlinks or open attachments until the legitimacy and safety of the communication has been properly verified and vetted.

1.3 Dangling Subdomain Hijacking

From a limited sample of cloud services and DNS records, researchers at Certitude have identified more than 1,000 subdomains of legitimate organizations which use DNS CNAMEs to point to cloud service hostnames/subdomains which no longer exist. By registering new services which re-use the target subdomains the researchers were able to host whatever content they chose and make it accessible via the legitimate organization subdomain.

A CNAME is a type of DNS record which indicates that a domain is an alias for another domain name. It is very common for organizations to use external cloud service providers to host websites and services. When those services are being accessed via a subdomain of the organizations primary DNS domain, that subdomain will typically be set up as a CNAME alias, with the true name/destination being a subdomain of the cloud service provider. When that service is discontinued, if the CNAME is not deleted, it will be left in what is known as a dangling configuration, where it points to a non-existent domain.

The research found many service providers freely allow the re-use, or re-registration of lapsed subdomains, and as such an attacker could identify a subdomain on a service provider which is pointed to by a CNAME of an organization, then host whatever content they wish on that service provider, which will be accessible via a sub-domain of a legitimate organization. This could then be used for phishing and social engineering, or to host malicious files which will appear to content filters to come from a benign/legitimate source.

WithSecure™ Insight

CNAME hijacking is not a technical attack, and it is also not a new attack, however the almost universal use of cloud services provides a much larger pool of possible targets. In addition, many cloud service providers have no controls around the re-use of lapsed sub-domains, which enables this sort of hijacking. From the perspective of internal organizations, dangling CNAMEs may not be recognized as a security issue, and so tidying up dangling DNS configurations may not be prioritized. WithSecure's Attack Surface Monitoring team regularly encounters subdomain takeover risks that have already been taken over and are serving attacker-controlled pages. In most cases it's generic advertising, online casinos etc. but it could be something worse.

What can you do?

Any organization that accesses external cloud or web services via a CNAME subdomain of the organizational domain name is at risk. Best practice is that organizations delete CNAMEs when the resource they point to no longer exists.

We recommend organizations see if they can use existing alerting within Azure Security Centre / AWS GuardDuty for dangling DNS detection / dangling S3 detection. Most subdomain takeover detection is reliant on a corpus of known takeover signatures. While a proven Attack Surface Management service is advised, organizations can easily self-assess themselves with tools such as DNSReaper. It is important to note subdomain takeovers can exist outside of known signatures, novel ones can exist and knowing what to look for is essential.

Organizations should also be aware that subdomain takeover detection is prone to false-positives due to the nature of cloud services. Whilst a subdomain may appear like it is dangling, if the service/profile still exists in an organization's cloud environment but is not associated with a resource, you cannot take it over, but it will appear vulnerable.

1.4 Juniper vulnerability mis-scored

VulnCheck has published research into an exploit of CVE-2023-36845, a vulnerability present in **Juniper SRX Firewalls** and **EX Switches**.

Juniper released a patch for CVE-2023-36845 (and others) at the beginning of September, but the vulnerability only received a 5.3 MEDIUM CVSS score, which broadly suggested a low risk of exploitation by a remote attacker.

The research and proof of exploit published by VulnCheck demonstrates that this CVSS score is inaccurate, and exploitation can be carried out by a remote attacker to achieve remote code execution (RCE), massively increasing the risk of exploitation associated with the vulnerability.

The fact that this vulnerability appears to have an inaccurate CVSS score may mean that it needs to be re-triaged by vulnerability management teams/personnel and risk revaluated.

Public scanning of internet facing instances of the vulnerable products show about 80% are unpatched and therefore vulnerable to exploit. Exploitation of this vulnerability is likely to occur.

This exploit is a development of a previous technique uncovered by watchTowr.

While the previous version required the upload of files to work, this new variation by VulnCheck uses Standard Input (stdin) instead. They say:

The affected firewalls run FreeBSD, and every FreeBSD process can access their stdin by opening /dev/fd/0. By sending an HTTP request, we're able to introduce a "file", /dev/fd/0, to the system.

Using that trick, we can set the PHPRC environment variable to /dev/fd/0 and include the desired php.ini in our HTTP request. The following curl request demonstrates this attack to prepend /etc/passwd to every response.

VulnCheck further developed this by abusing the "auto_prepend_file" string, to include a second malicious php source in their exploit.

WithSecure™ Insight

Firewalls are an attractive target for a myriad of threat actors, as they serve as the gateway for secure networks, and can allow possible traversal into other systems and storage to be further exploited or acted upon. The searches to identify vulnerable instances are simple and can be carried out on mass scanning services like Shodan, making targeting trivial. While this exploit involves multiple steps, the released exploit code now makes it easy to achieve RCE. It is highly likely that mass exploitation of these vulnerable devices will be carried out.

What can you do?

Scans suggest that approximately 80,000 internet facing vulnerable firewalls are vulnerable to the exploit. However, it is important to note that these figures can be skewed due to the presence of honeypots.

Juniper has provided advice and a patch to resolve this issue. You can also examine your "httpd.log" file for anomalous activity, such as:

```
httpd: 2: POST /?PHPRC=/dev/fd/0 HTTP/1.1
```

1.5 Hacktivism Updates

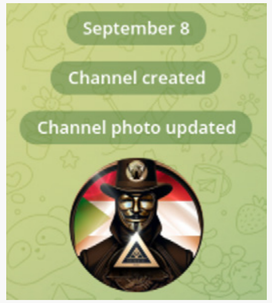
Oh Canada
Canada has come under fire from hacktivist groups following the visit of Ukrainian president Volodymyr Zelenskyy and a very unfortunate and well publicized incident where members of its House of Commons were encouraged to honor a war veteran who later turned out to have been a member of a Nazi SS regiment.

The activity includes DDoS activity by NoName057(16), which disrupted passport control services for Canada's border services agency, as well as an unattributed breach involving Air Canada which it states involved access to "*limited personal information of some employees and certain records*".

NoName057(16)
NoName057(16) continues to target numerous countries and businesses, including: Albania, Bulgaria, Canada, Croatia, Czechia, Denmark, Estonia, Finland, Germany, Latvia, Lithuania, Spain, Sweden, and the UK. With a focus on the transportation, financial, government and media sectors, this is in-line with the group's typical targeting and modus operandi.

Geopolitically, any perceived support for Ukraine or negative Russian sentiment is a catalyst for NoName057(16) attacks, as such they can often be predicted based upon news stories or changes within the landscape, even if it's just a refusal to play football against Russian football teams, which is what motivated the most recent attacks against the UK.

Anonymous Sudan
In a very strange chain of events Anonymous Sudan has targeted Telegram itself, due to having its channel deleted by the platform. Telegram has not provided a reason for deleting the @anonymoussudan channel, but it likely relates to the use of bots to inflate channel numbers. Unfortunately, this hasn't stopped the group's activity and the group has created a new channel which has quickly gained traction.



2 Ransomware: Trends and notable reports

The following data is limited to multi-point of extortion ransomware leak sites that are parseable and captured between 28th August 2023 and 28th September 2023.

This month has seen a significant (+45%) increase in overall activity, mainly attributable to newcomers **LostTrust, 3AM** and **CiphBit**, but also boosts in numbers across several groups, who it appears have returned from their summer vacations!

Despite last month's news regarding internal turmoil at **LockBit**, the group still dominates the ransomware landscape.

Clop made waves this year with the mass exploitation of vulnerabilities and leaks of huge volumes of victim data has only posted one victim to their leak site in September. Apparent Conti and **Royal** spin-off group **BlackSuit** also only posted one victim in September, suggesting that current and former Conti members are likely focusing on other initiatives.

Group	Victims	Percentage	Change
LockBit	127	23 %	37 %
LostTrust	52	10 %	New
Alphv	49	9 %	48 %
Ransomed	35	6 %	338 %
Cactus	33	6 %	Returned
NoEscape	26	5 %	24 %
Play	26	5 %	30 %
8Base	24	4 %	-17 %
Akira	18	3 %	-42 %
Medusa	13	2 %	8 %
BianLian	11	2 %	10 %
INC Ransom	11	2 %	267 %
Knight	10	2 %	900 %
3AM	10	2 %	New
Ragnar Locker	8	2 %	700 %
Trigona	8	2 %	Returned
CiphBit	8	2 %	New
Rhysida	7	1 %	-36 %
BlackByte	6	1 %	500 %
Other	60	11 %	N/A
Total	**542**		**45 %**

2.1 Do not pay says United States

The White House is urging countries not to pay ransoms to cybercriminals. The International Counter Ransomware Initiative (CRI) is a group of countries that are working together to combat ransomware. The CRI is expected to issue a joint statement in October urging members not to pay ransoms. Some experts support the plan, while others worry that it will not be effective.

There are several reasons why it is important avoiding paying ransoms to cybercriminals. First, paying ransoms encourages cybercriminals to continue attacking organizations. Second, it can be difficult to ensure that cybercriminals will actually decrypt an organization's data, even after a ransom is paid. Third, paying ransoms can fund further criminal activities.

However, there are also some challenges to not paying ransoms. For example, organizations may be concerned about the impact of a ransomware attack on their business operations or reputation. Additionally, governments may face political pressure to pay ransoms to restore critical services.

Overall, the White House's call for countries to stop paying ransoms to cybercriminals is an important step in the fight against ransomware. However, it is important to be aware of the challenges that organizations and governments face in implementing this policy.

2.2 Casino attacks

Following a cyber-attack, MGM resorts has had to shut down for about 10 days, likely costing the company well over $80 million dollars in lost revenue. The 10-day shut down was reportedly the result of MGM attempting to prevent the spread and damage of the attack, which has since been claimed by the ransomware group **Alphv**. On the 14th of September, Alphv posted on its leak site, stating that it had compromised MGM's Okta instance, but had not deployed ransomware when MGM shut down critical systems. This this did not deny the group's foothold, and it then went on to encrypt more than 100 ESXi instances and further claim that it still had access to MGM's network.

All of this news is being discussed at the same time that it has been revealed that another casino and resort in Las Vegas, Caesars Entertainment, paid a $15 million dollar ransom to avoid its data being leaked by an unnamed ransomware group.

These attacks are clear evidence of "big game hunting" by ransomware groups, striking high value targets who are far more likely to pay ransoms due to the reputational and financial damage caused by outages and data leaks. The decision by Alphv to make a statement regarding MGM and its response is an example of how ransomware groups can cause damage well beyond the initial attack, seeking to harm the reputation and belittle the response of defenders.

2.3 8Base uncovered?

8Base, which has been dumping victim data on its .onion leak site since late May 2023 has experienced a data leak of its own, which may have exposed one of the group's developers.

This investigation arose when a researcher was able to force an error by submitting a GET request to 8Base's chat feature. Exposed in the error message were the host IP address for the website (95.216.51[.]74) and a Gitlab server associated with an entity called **Jcube-gr** (gitlab[.]com/jcube-group/clients/apex/8base-v2). This Gitlab contains resources which were in-use on 8Base's site, including two PHP pages.

The owner of the Gitlab is a resident of Moldova called Andrei Kolev, who has denied any knowledge or interaction with 8Base when approached for comment. While it is not uncommon for developers to be unwittingly drawn into working for ransomware groups, what is highly suspicious is that 8Base's website was very quickly altered to remove the Jcube-gr materials, suggesting someone tipped 8Base off about the connection.

2.4 Gold Melody

Researchers from SecureWorks have produced an excellent article on the IAB Gold Melody. They describe Gold Melody as:

“a financially motivated group has been active since at least 2017, compromising organizations by exploiting vulnerabilities in unpatched internet-facing servers. The victimology suggests opportunistic attacks for financial gain rather a targeted campaign conducted by a state-sponsored threat group for espionage, destruction, or disruption”.

The tools used by Gold Melody fit within the well-known initial access playbook, but of particular note is the group’s exploitation of the following vulnerabilities:

- Log4Shell (CVE-2021-44228)
- JBoss MQ Java (CVE-2017-7504)
- Oracle WebLogic (CVE-2020-14882, CVE-2020-14750)
- Citrix ShareFile (CVE-2021-22941)
- Sitecore Server (CVE-2021-42237)
- Apache Struts (CVE-2017-5638)

The takeaway from this, is that defenders should have good coverage from the TTPs used by actors like Gold Melody, as they conform to well-known playbooks. Organizations must also concentrate on patch management, as high-risk vulnerabilities give attackers easy routes into an organization.

2.5 Real world impact

The real world impact of cyber-attacks is well known, with ransomware attacks being linked to deaths, and companies facing huge financial implications that can often be long lasting and hard to recover from.

UK logistics company KNP is an unfortunate example of this, with the firm announcing it has gone into administration and had to layoff 730 employees, following a ransomware attack earlier in the year carried out by Akira.

Another example of the risk of data leaks has been discussed by the UK’s information commissioner’s office (ICO), which states that leaked personal identifiable information (PII) can genuinely put lives at risk, especially in cases of domestic abuse or stalking, driving home the importance of proper data handling and risk mitigation.

2.6 Ransomware newcomers

3AM
A new ransomware variant and group called 3AM has struck victims and posted victim data on its dark web leak site since the 17th of September. Interestingly, in one known instance an attacker deployed 3AM after failing to deploy LockBit suggesting the attacker was an affiliate in both groups.

Retch
Little is known about newcomer Retch but its ransom note demands a relatively low amount of €300, suggesting it is targeting small businesses or consumers, rather than bigger organizations.

S.H.O
Another new variant that appears to be targeting small businesses and consumers is S.H.O. Similarly, to Retch, this group is demanding a small ransom of $200.

Lost Trust
LostTrust has posted 52 victims to its dark web leak site, a huge number that was all dumped on the same date, suggesting a longer campaign. This aligns with reports that LostTrust is a simple rebrand of **MetaEncryptor**, with the groups utilizing the same website templates and encryption locker.

CiphBit
Intelligence on CiphBit is scant, but the group dumped data relating to eight different victims on its dark web leak site in September. These victims come from different nations (Canada, Belgium, France, Germany, Moldova, Poland, and the UK) and different sectors, suggesting the group is purely opportunistic, rather than motivated by a specific target characteristic or ideology.

3 Other notable highlights in brief

3.1 SilentScraper

Researchers at BlackBerry have uncovered a new payment data scraping campaign, which they report has been active over a year. They have dubbed the campaign/actor SilentScraper and suggested that the attackers are Chinese language users. The group behind SilentScraper target vulnerable web applications, with the intention of compromising web store checkout pages so that sensitive payment data can be captured and exfiltrated. Noteworthy is the belief that the attackers are shifting their targeting to organizations within North America, while previously focusing on victims in Asia.

3.2 R1Z EDR killer

We have previously reported on the malware marketed as **SpyBoy Terminator**, which describes itself as an "EDR killer". There are reports that a new threat actor has advertised a proof-of-concept for a new "EDR killer" called **R1Z**. Their demonstration shows its use against CrowdStrike's Falcon product, but other EDR agents are mentioned in the malware's advertisement, including Sophos, SentinelOne, MS Defender, Trend Micro, and indeed F-Secure/WithSecure™, among many others.

WithSecure™ use a layered approach in dealing with similar Bring Your Own Vulnerable Driver (BYOVD) exploits, which involves:

- Detections matching against known vulnerable drivers.
- Detections for driver additions to hosts, or drivers being loaded by hosts.
- WithSecure™ combine those alerts with several factors and behavioral detections to improve context and adjust detection severity and respond accordingly.

3.3 LastPass crypto wallets wiped

Tayor Monahan of crypto wallet company MetaMask has uncovered a connection between 150 different victims of crypto theft, being that they all had stored their recovery "seed phrase" within the LastPass password manager. Unfortunately for the victims, LastPass experienced a large scale compromise in November 2022, which resulted in the breach of both encrypted and plaintext data, which it appears has been used to access their crypto wallets. The collective sum of the theft is about $35 million, and the victims appear to be well established crypto investors. This incident serves as a stark reminder that breaches can be weaponized to cause real impact, and that if you suspect a breach of your data has occurred you must take measures to secure any service that relied upon the security of that data, seed phrases included.

4 Threat data highlights

4.1 Vulnerabilities & Exploits

Vulnerabilities of note

Progress WS_FTP
CVE-2023-40044, CVE-2023-42657 (and 6 others)

Several vulnerabilities have been discovered in Progress' WS_FTP services, with one scoring a perfect 10 CVSS score, and another scoring 9.9, making them CRITICAL. Because some of these vulnerabilities are CRITICAL, and this type of file service is a highly attractive target for data theft/ransomware actors, it is likely that these vulnerabilities will be exploited in the immediate future. Fixes are available via Progress and should be installed as soon as practicable.

Libvpx video library
CVE-2023-5017

It has been confirmed that "a commercial spyware vendor" has been actively exploiting this vulnerability. Libvpx is a widely used video codec, present in multiple operating systems, web browsers, applications and code bases. The libvpx video library is found in any application, operating system, or code library that supports the VP8 and VP9 video format. While it is only a single vulnerability, the library can and most likely will be present independently in multiple applications on the same device, and each vulnerable application will need to be individually patched. The vulnerable library is implemented on Windows, as well as iOS, Android, and other Unix based operating systems such as Linux and BSD. It has been confirmed that "a commercial spyware vendor" has been actively exploiting this vulnerability.

WebP image library
CVE-2023-5129 *(this vulnerability was somewhat erroneously reported under multiple CVEs)*

There is an actively exploited Zero-day vulnerability in the WebP image library. This is very similar to the aforementioned libvpx vulnerability. The WebP image library is found in any application, operating system, or code library that supports the WebP format, which includes all Electron based apps, most major browsers, and many other applications used by enterprises and applications.

Microsoft SharePoint
CVE-2023-29357, CVE-2023-24955

At the Pwn2Own hacking event, researchers demonstrated a chaining of 2 vulnerabilities to achieve RCE on vulnerable SharePoint instances. Since the demonstration, a proof-of-concept has been released that makes in-the-wild exploitation highly likely. Microsoft have released updated versions of SharePoint which rectify the issues but relies upon organizations patching in a timely manner.

Exim
CVE-2023-42115

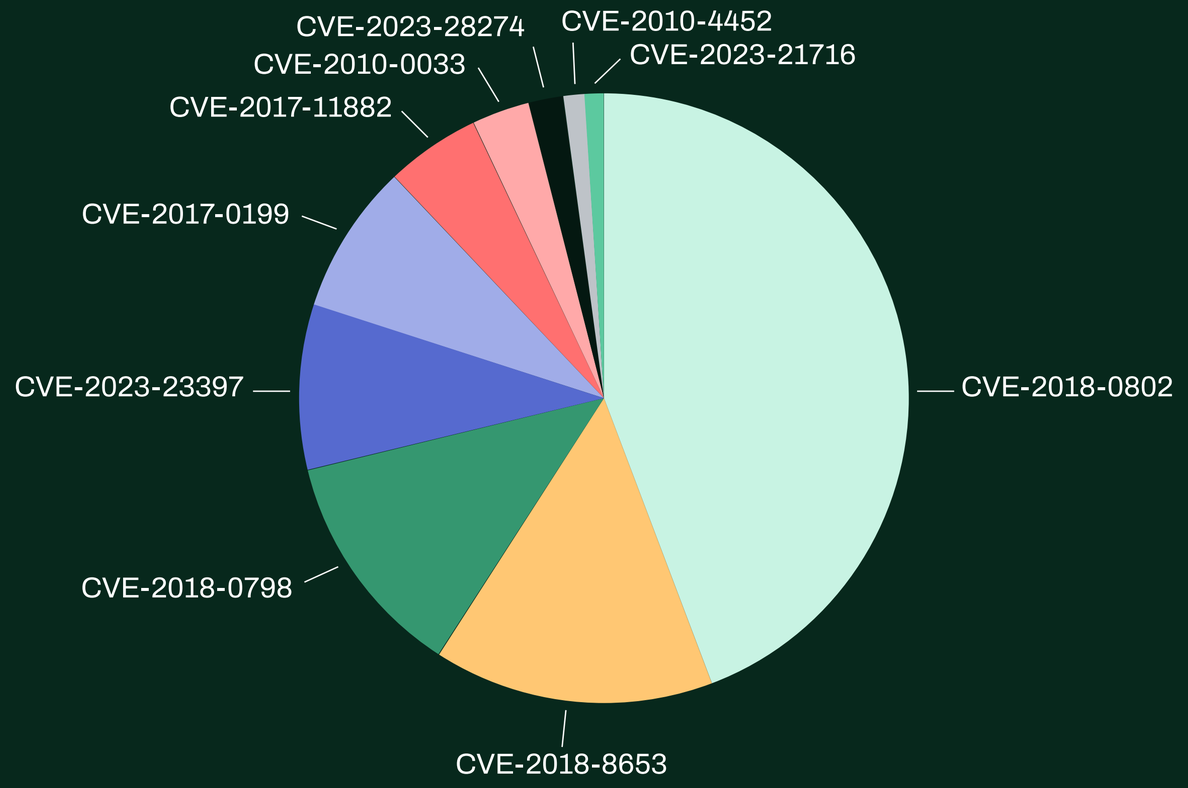
A vulnerability in Exim has been reported via the zero-day initiative platform, which has scored a CVSS score of 9.8. The vulnerability can be exploited by a remote and unauthenticated attacker to achieve RCE, which would make it an attractive weapon in any attacker's arsenal. At present, Exim has addressed 3 out of 6 vulnerabilties.

What have we seen?

This data is taken from WithSecure's EPP (EndPoint Protection) telemetry, and relates to detections of LOCAL vulnerabilities, typically delivered as part of malware. Remote/network exploitation of edge services are not in scope.

These vulnerabilities are well-established and well-known, highlighting that most threat actors and attackers favor weaponizing their binaries with proven exploits. 90% of the vulnerabilities relate to Windows devices, and 70% involve Microsoft Office applications, showing a preference for targeting these devices and applications. This is likely due to their prevalence, but also because Office vulnerabilities are easier to target via common vectors such as phishing and malvertising.

The top 10 vulnerabilities witnessed in our EPP telemetry this month are as follows:



What vulnerabilities are being newly exploited?

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

CVE ID	Vendor / Product	CVSS Rating	What's the vulnerability?
CVE-2023-33246	Apache RocketMQ	CRITICAL	"Several components of Apache RocketMQ, including NameServer, Broker, and Controller, are exposed to the extranet and lack permission verification. An attacker can exploit this vulnerability by using the update configuration function to execute commands as the system users that RocketMQ is running as or achieve the same effect by forging the RocketMQ protocol content."
CVE-2023-20269	Cisco Adaptive Security Appliance	CRITICAL	"Cisco Adaptive Security Appliance and Firepower Threat Defense contain an unauthorized access vulnerability that could allow an unauthenticated, remote attacker to conduct a brute force attack in an attempt to identify valid username and password combinations or establish a clientless SSL VPN session with an unauthorized user."
CVE-2021-3129	Laravel Ignition	CRITICAL	"Laravel Ignition contains a file upload vulnerability that allows unauthenticated remote attackers to execute malicious code due to insecure usage of file_get_contents() and file_put_contents()."
CVE-2023-41993	Apple	CRITICAL	"Apple iOS, iPadOS, macOS, and Safari WebKit contain an unspecified vulnerability that can allow an attacker to execute code when processing web content."
CVE-2018-14667	Red Hat Jboss RichFaces Framework	CRITICAL	"Red Hat JBoss RichFaces Framework contains an expression language injection vulnerability via the UserResource resource. A remote, unauthenticated attacker could exploit this vulnerability to execute malicious code using a chain of Java serialized objects via org.ajax4jsf.resource.UserResource$UriData."
CVE-2023-41064	Apple	HIGH	"Apple iOS, iPadOS, and macOS contain a buffer overflow vulnerability in ImageIO when processing a maliciously crafted image, which may lead to code execution. This vulnerability was chained with CVE-2023-41061."
CVE-2023-41061	Apple	HIGH	"Apple iOS, iPadOS, and watchOS contain an unspecified vulnerability due to a validation issue affecting Wallet in which a maliciously crafted attachment may result in code execution. This vulnerability was chained with CVE-2023-41064."
CVE-2023-36802	Microsoft Streaming Service Proxy	HIGH	Microsoft Streaming Service Proxy contains an unspecified vulnerability that allows for privilege escalation.
CVE-2023-35674	Android	HIGH	Android Framework contains an unspecified vulnerability that allows for privilege escalation.
CVE-2023-4863	Google Chromium WebP	HIGH	"Google Chromium WebP contains a heap-based buffer overflow vulnerability that allows a remote attacker to perform an out-of-bounds memory write via a crafted HTML page. This vulnerability can affect applications that use the WebP Codec."
CVE-2023-26369	Adobe Acrobat/Reader	HIGH	Adobe Acrobat and Reader contains an out-of-bounds write vulnerability that allows for code execution.
CVE-2022-22265	Samsung Mobiles	HIGH	"Samsung devices with selected Exynos chipsets contain a use-after-free vulnerability that allows malicious memory write and code execution."
CVE-2014-8361	Realtek SDK	HIGH	"Realtek SDK contains an improper input validation vulnerability in the miniigd SOAP service that allows remote attackers to execute malicious code via a crafted NewInternalClient request."
CVE-2017-6884	Zyxel EMG2926	HIGH	"Zyxel EMG2926 routers contain a command injection vulnerability located in the diagnostic tools, specifically the nslookup function. A malicious user may exploit numerous vectors to execute malicious commands on the router, such as the ping_ip parameter to the expert/maintenance/diagnostic/nslookup URI."
CVE-2022-31462	Owl Labs Meeting	HIGH	"Owl Labs Meeting Owl contains a use of hard-coded credentials vulnerability that allows an attacker to control the device via a backdoor password (derived from the serial number) that can be found in Bluetooth broadcast data."
CVE-2022-31463	Owl Labs Meeting	HIGH	"Owl Labs Meeting Owl contains an improper authentication vulnerability that does not require a password for Bluetooth commands, as only client-side authentication is used."
CVE-2023-28434	MinIO	HIGH	"MinIO contains a security feature bypass vulnerability that allows an attacker to use crafted requests to bypass metadata bucket name checking and put an object into any bucket while processing `PostPolicyBucket` to conduct privilege escalation. To carry out this attack, the attacker requires credentials with `arn:aws:s3:::*` permission, as well as enabled Console API access."
CVE-2023-41179	Trend Micro Apex One	HIGH	"Trend Micro Apex One and Worry-Free Business Security contain an unspecified vulnerability in the third-party anti-virus uninstaller that could allow an attacker to manipulate the module to conduct remote code execution. An attacker must first obtain administrative console access on the target system in order to exploit this vulnerability."
CVE-2023-41992	Apple	HIGH	Apple iOS, iPadOS, macOS, and watchOS contain an unspecified vulnerability that allows for local privilege escalation.
CVE-2023-36761	Microsoft Word	MEDIUM	Microsoft Word contains an unspecified vulnerability that allows for information disclosure.
CVE-2022-31459	Owl Labs Meeting	MEDIUM	"Owl Labs Meeting Owl contains an inadequate encryption strength vulnerability that allows an attacker to retrieve the passcode hash via a certain c 10 value over Bluetooth."
CVE-2022-31461	Owl Labs Meeting	MEDIUM	"Owl Labs Meeting Owl contains a missing authentication for critical functions vulnerability that allows an attacker to deactivate the passcode protection mechanism via a certain c 11 message."
CVE-2023-41991	Apple	MEDIUM	"Apple iOS, iPadOS, macOS, and watchOS contain an improper certificate validation vulnerability that can allow a malicious app to bypass signature validation."

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