Threat Highlight Report

January 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 GoTo breach, the resurgence of Emotet, the prevalence of malware being distributed via Google search results, and a look at malware designed to target Apple devices throughout 2022.

We look at the ransomware landscape, including the most prevalent hack/leak actors from January, LockBit's (or at least one of their affiliates') attack on the UK Royal Mail postal service, BianLian's new I2P leak site, an interview with the criminals behind Mallox and a look at newcomers CatB.

We also discuss the Nordic common cybersecurity strategy, the leaks of Cellebrite and MSAB data, a technical look at the OWASSRF exploit, more on Russian hacktivist groups and their activity in Poland and Denmark, crypto freejacking and examine Kela's 2022 cybercrime report.

As ever, we look to WithSecure's telemetry for insight into malware observed, and the top vulnerabilities exploited in the wild as seen by WithSecure™ and CISA's telemetry.

- Ziggy Davies, Threat Intelligence Analyst

1 Monthly highlights

1.1 GoTo (LogMeIn) breach

Last month, we wrote about the breach of data storage belonging to LastPass, which resulted in the compromise of customer's data and passwords (encrypted), and it now appears that the company's parent organization GoTo (formerly called LogMeIn) was part of the same breach and has described the data storage as "*a third-party storage facility*".

It appears that the data which has been compromised is a backup and includes:

- GoTo Central and Pro usernames
- GoTo Central and Pro passwords (salted and hashed)
- Deployment and provisioning data
- One-to-many scripts
- Multi-factor authentication information
- Account PII including the last 4 digits of credit cards
- An encryption key for a portion of the stolen data

GoTo has reset passwords and informed customers directly about the breach, but given this breach began in November, communication has certainly been lacking.

WithSecure™ Insight

We now know that the cloud service which was breached as part of the LastPass compromise, also contained the above-mentioned data for GoTo. At the time of writing there's no mention of whether any other companies are involved.

While GoTo has taken appropriate security measures in salting and hashing the stored passwords, it is alarming that materials relating to encryption algorithms were also able to be stolen, potentially making decryption of certain data trivial, though GoTo have failed to clarify which data the encryption key relates to.

Our advice, as with any compromise, is as follows:

- Change passwords
- Consider changing account usernames and email addresses, as these are now leaked
- Prepare for an increase in phishing activity linked with the leak of email addresses and PII
- Prepare for social engineering attacks designed to elicit information that may allow further abuse of the compromised data

1.2 The rise of Emotet (again)

In November 2022's WithSecure Threat Highlight Report, we included a brief mention of Emotet's return following a 5-month hiatus. It now seems that Emotet is in full swing, with Cofense Intelligence reporting updates to Emotet's loader DLL's and BlackBerry detailing Emotet's new TTPs.

These new TTPs were discussed in November by Proofpoint and involve:

- Use of new visual lures, excel attachments, and inclusion of specific instructions on how to open the file (*and detonate the malware*).
- Changes to the Emotet binaries.
- Usage of further payloads, which include IcedID and Bumblebee.

WithSecure™ Insight

The observations of Cofense, BlackBerry, and Proofpoint all align with our own insights and telemetry, with a significant rise in Emotet-related activity occurring since November 2022.

For the most part, the activity being seen is traditional Emotet activity, but the social engineering aspect of recent Emotet attacks is quite interesting and includes the use of specific instructions on how to open the malicious Emotet .xls files:

```
In accordance with the requirement of your
security policy, to display the contents of
the document, you need to copy the file to
the following folder and run it again:

for Microsoft Office 2016 x64 and later – C:\
Program Files\Microsoft Office\root\Templates
```

Doing so allows the documents macros to detonate immediately upon opening, bypassing Microsoft's Mark-of-the-Web (MOTW) flag which would ordinarily trigger protected view and disable macros.

The best way to protect against Emotet, is the use of email filtering and rules, the use of security products, especially those that detect suspicious behaviors, by disabling Macro's by adjusting group policy settings, as well as training end-users in how to detect phishing/malicious office documents.

1.3 SEO poisoning at an all-time high

Search Engine Optimization (SEO) poisoning, which is a malware delivery technique that involves getting malicious websites ranked or advertised in Google search results is reportedly at an all-time high. The plethora of malware strains using Google search results as a delivery mechanism includes:

- Gootkit
- Gootloader
- IcedID
- BATLOADER
- PrivateLoader
- NullMixer
- RedLine infostealer
- Rhadamanthys stealer
- VIDAR stealer
- Yellow Cockatoo's RAT
- VagusRAT

The technique involves the inclusion of specific SEO keywords that result in threat actors' malicious websites being pushed towards the top of Google search results, or alternatively, threat actors actually paying Google to get themselves to the 'Ad' top section of results, something which has been witnessed on numerous occasions.

Public frustration in Google's response time and success of such campaigns may suggest a continuation of actors utilising this technique, at least in the short term.

WithSecure™ Insight

The abuse of Google search results to direct victims to malicious websites and deliver malware is something that has been occurring for a long time, that we have reported on numerous times within our Threat Highlight Report. Unfortunately, it appears that this technique has grown to be the preferred delivery mechanism for many actors, and this is likely because:

- It's non-technical, and therefore easy to set up.
- It's cheaper to set up than a spam delivery network.
- It's very common for people to search for websites/software and click the first result rather than input the full address in their browser.
- By imitating high-profile brands/typosquatting threat actors are able to drive victim interaction.
- Google appears to be slower to respond to takedown requests than automated spam filtering, allowing malicious search results to appear for a longer time.
- Good use of email filtering/rules and education around phishing have hampered the effectiveness of spam campaigns.

The best way to combat this technique is appropriate user education and training surrounding the use of search engines, and the use of appropriate security products that can detect malicious in-browser activity.

1.4 Mac malware of 2022

Patrick Wardle of Objective-See, has produced an excellent write-up regarding new malware which was seen during 2022, that specifically targets MacOS.

The article breaks down 13 new malware strains, by looking at:

- Infection vectors
- Persistence mechanisms
- Features of the malware and its goals
- Specific indicators of compromise

The 13 variants examined include:

- SysJoker: A simple cross-platform backdoor
- DazzleSpy: A feature-rich implant, deployed via Safari
- CoinMiner: A cryptocurrency miner
- Gimmick: A multi-platform feature-rich implant, that leverages the cloud for C2.
- oRat: An implant used by the threat actor Earth Berberoka
- CrateDepression: Spread via typosquatting
- Pymafka: Spread by typosquatting, installs Cobalt Strike
- Covid: A backdoor that can execute further payloads
- CloudMensis: Primarily used as a stealer
- rShell: Often delivered via the supply-chain, this is a basic RAT
- Insekt: Part of the Alchimist framework, with Insekt payloads being available for macOS
- KeySteal: A keychain stealer embedded in “free” software
- SentinelShark: Another malware spread by typosquatting that is used as a stealer

WithSecure™ Insight

The device management company Jamf, which creates products designed to manage Apple devices in enterprise environments, is witnessing rapid and continual growth in the use of Apple devices in the workplace, with growth occurring over the past 2 years.

The reasoning for this is likely the release of M1/M2 powered machines, along with decent affordability/performance characteristics, as well as a desire for more portable devices due to an increase in work-from-home practices following the pandemic.

This rise in usage has resulted in a comparable rise in the creation and adoption of malware designed to target MacOS, including the newer ARM M1/M2 machines (SilverSparrow, SysJoker), as noted by Patrick Wardle in their excellent reporting.

There is a common misconception that Apple devices are somehow free from abuse/malware. Unfortunately, that’s not true as a myriad of malware is available for MacOS, and Apple is no stranger to the need for regular security updates. It’s clear that the increase of Apple in enterprise environments will be met with a parallel rise in threat actors targeting Apple devices, operating systems, and software.

2 Ransomware: Trends and notable reports

A new year, but the same story regarding ransomware in January with LockBit leading the ransomware attack landscape by far, but with newcomers Royal and Play continuing to be highly prevalent.

The following data is limited to ransomware leak sites which are parsable and was captured between 1st January 2023 and 23rd January 2023.

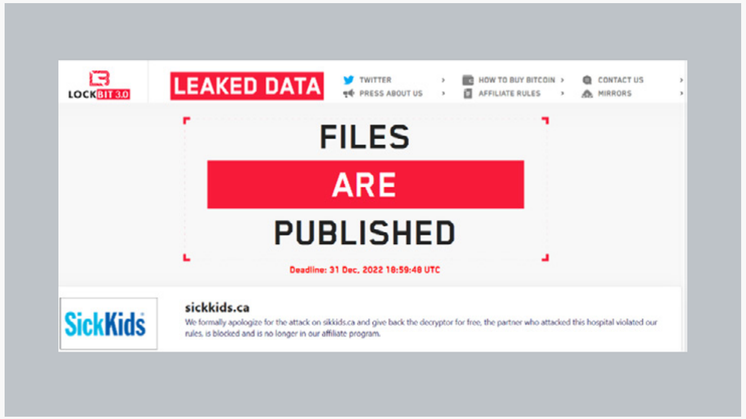
Group	Victims	Percentage
LockBit 3.0	27	22%
Royal	15	12%
Vice Society	13	11%
Alphv (BlackCat)	13	11%
Play	11	9%
Clop	10	8%
BlackByte	6	5%
BlackBasta	4	3%
Mallox	4	3%
Lorenz	3	3%
Hive	3	3%
RansomHouse	3	3%
BianLian	3	3%
Everest	1	<1%
Snatch	1	<1%
Nokoyawa	1	<1%
Karakurt	1	<1%
0mega	1	<1%
Daixin	1	<1%

2.1 Royal Mail hit by LockBit… affiliate

On January 10th the United Kingdom's Royal Mail postal service was struck by a cyber-attack which was ultimately revealed to be a ransomware attack. The attack resulted in Royal Mail being unable to process international deliveries, with them delivering an update on the 23rd of January that services had resumed.

A leaked ransom note, apparently printed during the incident, suggests that the attack was perpetrated by LockBit, using their most recent "Black" or 3.0 variant. LockBit initially denied any involvement in the attack, but later confirmed a rogue affiliate had launched the attack without prior consent/permission. This is not the first time LockBit has blamed attacks on individual affiliates, with a recent attack on a children's hospital resulting in an apology and the release of the decryptor for free.

This confusion is due to the way LockBit apparently run their criminal enterprise, with affiliates having the ability to work semi-autonomously, but with guidance/rules regarding victimology.



No similar apology or decryptor has been released following the Royal Mail attack, but it certainly doesn't fit with their ordinary victimology, and will have likely caused a lot of tensions within the group, as hitting high-profile targets relating to national infrastructure is a quick way to instigate the wrath of government cyber departments such as GCHQ and National Cyber Force.

2.2 A history of LockBit

Chief Security Strategist Jon DiMaggio of Analyst1 has released an exceptional article titled "Ransomware Diaries: Volume 1". The article goes through the history of the LockBit ransomware group, its origins, development, internal issues, and leadership.

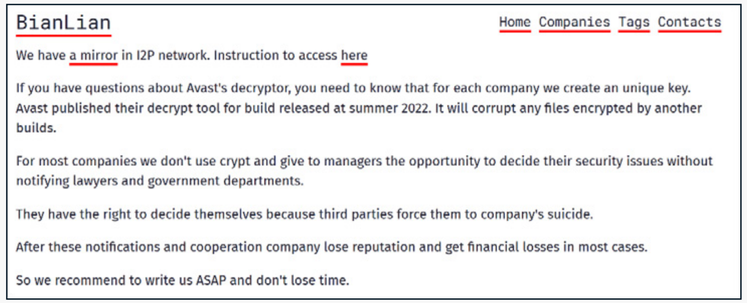
The key findings are:

- The leader of LockBit uses the persona LockBitSupp
- LockBitSupp regularly conducts smear campaigns against rival ransomware groups
- LockBitSupp allegedly keeps their PGP keys, crypto wallets and key files on two USB drives
- LockBitSupp allegedly uses Starlink to access the internet/ its infrastructure
- LockBit allegedly use crypto exchanges in Hong Kong to launder its money
- The developer of LockBit Black is also the developer of Dark-Side and BlackMatter
- LockBit has relationships with other ransomware groups such as DarkSide/BlackMatter, Alphv, REvil, Hive and BlackBasta
- LockBit alleges that Conti and now BlackBasta are support-ive of the Russian FSB

2.3 BianLian decryptor and shift to I2P

The ransomware group BianLian has recently had a decryptor released for one of their older variants, with the group keen to point out that they have since moved to a different build and the decryptor will no longer work.

The group has also diversified its leak site, and has created a mirror on the I2P network, something which is not common amongst ransomware groups but is a growing theme in dark web marketplaces due to growing issues over the seizure and disruption of .onion tor domains.



2.4 Newcomers: CatB

Ransomware newcomers CatB have undergone analysis thanks to Minerva-Labs.

The sample analyzed by Minerva appeared on VirusTotal in November 2022. It is notable as it contains several anti-VM techniques to ensure that it will only be executed on physical machines and uses DLL hijacking to try to evade detection.

2.5 An interview with Mallox

Mallox, a ransomware group who have been active since June 2021 has recently participated in a Q&A with @amvinfe, providing an unusual insight with the key points being:

- Mallox evolved from prior versions "TargetCompany" and "Fargo", was previously used by various groups, but was later purchased and became "Mallox" and now consists of only a few members.
- The members of Mallox belonged to another ransomware group, but felt they were not being paid fairly, and started Mallox.
- Mallox prefer to ask for smaller ransom demands than is typical, as they feel it is more likely to be paid.
- The group state they are not politically aligned, but admits they do not target Kazakhstan, Russia, Qatar, or Ukraine.
- The group is based in Europe.
- The group does not target hospitals or welfare-related businesses.
- They claim to have struck thousands of organizations, but only publish very few to their leak site, and limit the amount of data leaked to what is particularly interesting.
- The group is purely motivated by money.

3 Other notable highlights in brief

3.1 Nordic common cybersecurity strategy

Plans are moving ahead to create a defense-focused common cyber security strategy for the Nordic region, as part of NORDEFCO's vision 2025 initiative. The project is seen as a vital part of increasing the military capabilities and defenses of the involved nations, and comes at a time when the threat of cyberattack is at its highest, with several Nordic nations recently coming under attack from Russian-aligned groups.

3.2 Cellebrite & MSAB XRY data leaked

On the 13th of January 2023, an "*anonymous whistleblower*" sent data relating to forensic software from the companies Cellebrite and MSAB to the website 'Enlace Hacktivista'.

```
httpx://enlacehacktivista[.]org
```

This data was quickly picked up and shared on the leak site **Distributed Denial of Secrets** and is available for direct download or by torrent.

```
httpx://ddossecrets.substack[.]com/p/
cellebrite-msab-phone-forensics-leak\
```

Cellebrite, an Israeli company, produces a product called UFED which is a software package and hardware device, designed to access mobile devices, clone data from the device, and allow the user to analyze the data in an intuitive way. Cellebrite products are able to access both Apple and Android mobile devices, likely through the use of exploits, but the extent of this is kept secret by the company. MSAB is a Swedish company that produces a product called XRY, which is similar in functionality to Cellebrite.

Both companies provide their products and services to global customers, often from the law enforcement and intelligence sectors.

WithSecure™ can confirm the data as present and it appears to be legitimate.

This leak is likely to be problematic for any organization using Cellebrite or MSAB products, such as those working in:

- Law enforcement
- Intelligence
- Government
- Military, etc.

Previous data leaks have brought the forensic integrity of evidence gathered using such tools into question, as it has highlighted the potential for tampering or issues with the evidential chain of custody, which would be highly problematic for law enforcement.

These tools could also be potentially abused by hostile entities to invade privacy and gather evidence/intelligence on third parties. Though they would first need to be cracked.

No action is necessary at this time, if you are a user of either Cellebrite or MSAB XRY products, please contact your representative for advice. This is a developing news story of particular interest, and further information is likely to be available over time.

3.3 OWASSRF, a technical write-up

Viettel, who are the original finders of the vulnerabilities (CVE-2022-41080 and CVE-2022-41076) used in recent OWASSRF attacks by Play ransomware has released a technical analysis of the techniques.

The report is technical but may be useful to those wishing to research how OWASSRF attacks are undertaken and can potentially be detected.

3.4 Breach of Slack

On the 29th of December 2022, Slack were alerted to suspicious activity relating to their GitHub account. Slack's report states that an unknown threat actor gained access to their external GitHub account thanks to the theft of employee tokens (OAuth). While no customer data was involved, this does appear to part of a long and ongoing campaign that uses stolen access tokens in order to steal sensitive repo data.

3.5 Poland warns of Russian cyber attacks

Poland has released a statement relating to ongoing attacks by Russian-aligned groups on the nation due to Poland's support for Ukraine.

The report specifically mentions the hacktivist group NoName057(16) and a DDoS attack on the website of the Polish parliament, stating:

"*Data analysis showed that the website's unavailability was the result of an attack carried out by the pro-Russian group NoName057(16). This group on the Telegram portal has set the parliamentary website as one of its goals. This attack was a response to the adoption by the Sejm of the Republic of Poland of a resolution recognizing Russia as a state sponsor of terrorism.*"

There is also mention of a campaign designed to imitate legitimate Polish governmental websites, which are designed to harvest/phish data from Polish citizens and commit theft/fraud.

3.6 Denmark struck by Russian hacktivist DDoS

Speaking of pro-russian hactivism, on the 8th of December 2022 Denmark experienced a DDoS attack on a number of government websites, and a recent article has been critical of the response time, stating that it took 11 hours to resolve the matter.

These attacks are often organized via Telegram groups, and targets are often polled and decided ahead of time, potentially giving defenders a brief opportunity to anticipate attacks. Unfortunately, attacks of this nature are likely to continue while Russia continues to occupy Ukraine, and Russian narratives and disinformation paint allies of Ukraine and the wider NATO community as legitimate targets.

3.7 Freejacking

Freejacking is a form of cryptojacking that abuses free accounts on cloud services in order to perform cryptomining. Researchers at Unit 42 have detected an organized campaign designed to conduct freejacking by a threat actor they have dubbed Automated Libra. The key points from their report are:

- Automated Libra is abusing DevOps automation techniques in order to automate account creation and mining activities.
- At the peak of activity, the group was creating 3-5 GitHub accounts per minute.
- Automated Libra was able to bypass CAPTCHA images using simple image analysis techniques.
- More than 130,000 accounts were created in the campaign.
- Some of the accounts used stolen credit card information to create accounts, resulting in unpaid balances on fraudulent accounts.
- Unit 42 is calling this cryptojacking technique "Play and Run".

.

3.8 SugarCRM actively exploited

The customer relationship management system (CRM) Sugar, developed by the US company SugarCRM, has been under active attack thanks to a missing input validation error (CVE-2022-22952), which can result in RCE.

The vulnerability allows attackers to craft a request and inject custom PHP code via “EmailTemplates”, with proof-of-concept and valid exploits appearing online.

SugarCRM has released an advisory and has subsequently released patches fixing the issue.

3.9 Kela report on cybercrime in 2022

The team at intelligence company Kela have produced a comprehensive report titled “The State of Cyber Crime Threat Intelligence 2022”, which includes a survey of 426 security professionals involved in managing vulnerabilities in their workplace. The key findings of the report are:

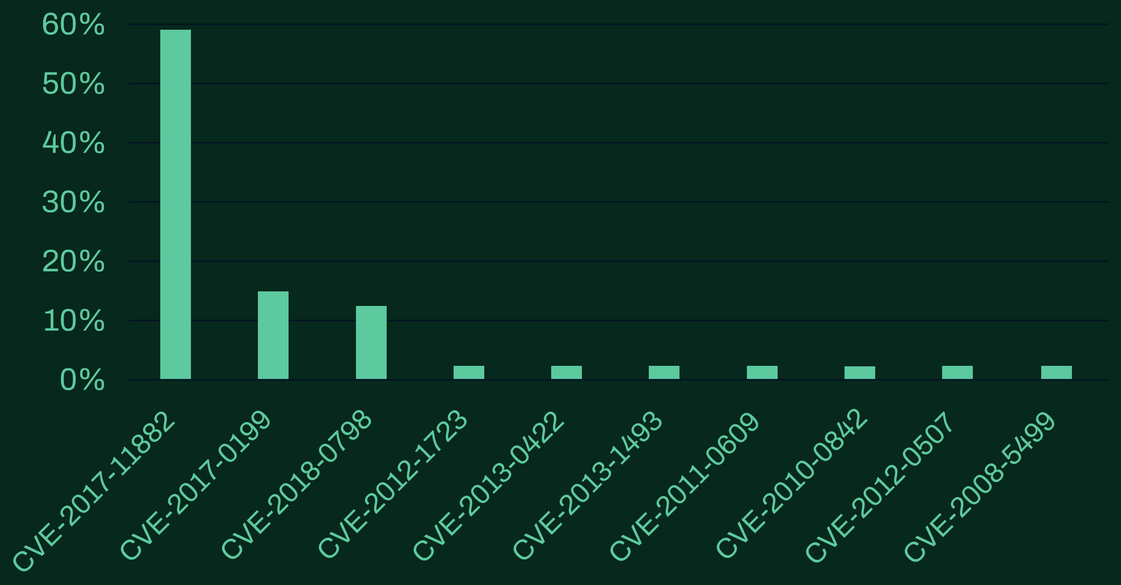
- Defenders need additional training and proficiency in performing investigations, which includes a method for identifying breaches and monitoring the criminal underground.
- Most survey respondents (69%) are concerned about their organizations data being released/sold on cybercrime forums.
- Only 38% of respondents believe they would detect the potential leaking/sale of their data within the criminal underground.
- 31% of respondents believe their current security program is not very effective.
- The biggest challenge is described as not having the tools or systems to investigate threats, as well as not having access/insight into the criminal underground.
- 49% of respondents are unhappy with their visibility into the criminal underground.

4 Threat data highlights

4.1 Exploits

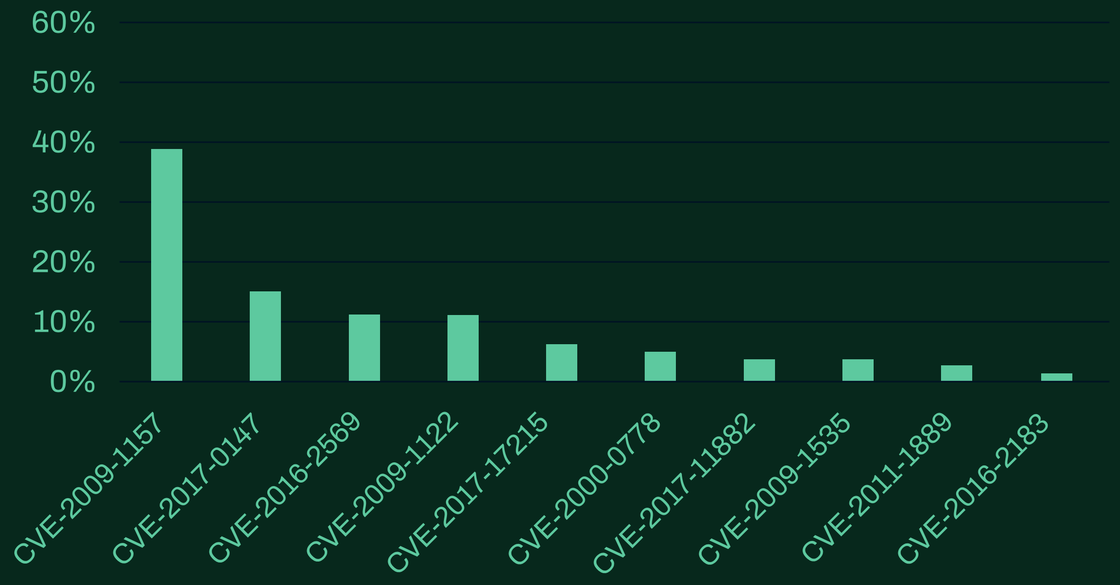
The following data was captured throughout January 2023.
There's little change across the vulnerability exploitation landscape again this month, with old favorites such as CVE-2017-1182, CVE-2017-0199 and CVE-2017-0147 all continuing to score highly, which are all vulnerabilities relating to Windows/Microsoft Office.

Top 10 exploits in the wild (WithSecure™ Telemetry)



WithSecure™ endpoint protection

Top 10 exploits in the wild (External Sources)



WithSecure™ endpoint protection

CISA’s known exploited vulnerabilities catalog

This month CISA have added 4 new exploited vulnerabilities to their catalog. 2 of which are rated as CRITICAL, and 1 in Zoho ManageEngine which is currently unrated but is likely to be CRITICAL, and is being actively exploited with proof-of-concept exploit code appearing online.

CVE ID	Vendor / Product	CVSS Rating	What's the vulnerability?
CVE-2022-47966	Zoho	Unrated (Likely Critical)	Multiple Zoho ManageEngine products contain an unauthenticated remote code execution vulnerability due to the usage of an outdated third-party dependency, Apache Santuario.
CVE-2022-44877	CWP	Critical	CWP Control Web Panel (formerly CentOS Web Panel) contains an OS command injection vulnerability that allows remote attackers to execute commands via shell metacharacters in the login parameter.
CVE-2022-41080	Microsoft	Critical	Microsoft Exchange Server contains an unspecified vulnerability that allows for privilege escalation. This vulnerability is chainable with CVE-2022-41082, which allows for remote code execution.
CVE-2023-21674	Microsoft	High	Microsoft Windows Advanced Local Procedure Call (ALPC) contains an unspecified vulnerability that allows for privilege escalation.

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