Threat Highlight Report

November 2023

WITH secure

Contents

1 Monthly highlights 3
2 Hacktivist landscape..... 5
3 Ransomware: Trends and notable reports..8
4 Other notable highlights in brief 11
5 Threat data highlights 13
6 Detection and response highlights 15

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, delivering an overview of this month's cybersecurity news, the changing threat landscape, and relevant advice.

This month's report is a little bit peculiar, as there is a lot of focus on the exploitation of vulnerabilities throughout. This is due to large and highly impactful campaigns recently that have involved exploitation, such as Citrix and Confluence. While this has skewed the content of our report somewhat, it helps reinforce how important patch management is, and demonstrates how quickly threat actors can capitalize on vulnerabilities. In summary, we look at the exploitation of SysAid, Citrix, Qlik Sense, Confluence, and an unnamed 0-day used to distribute Mirai.

We continue to track the ransomware landscape with statistics from known attacks and a look at newcomer Meow. We also reference our recent summative research on ransomware, which focuses on newcomers and overlap between groups.

Ziggy Davies
Intelligence Analyst

1. Monthly highlights

Lace Tempest targets SysAid

On the 2nd of November 2023, the security team at SysAid was alerted to a vulnerability in on-premises SysAid instances. This vulnerability was publicly disclosed on the 8th of November 2023 and is described as a “path traversal vulnerability leading to code execution” and is tracked as CVE-2023-47246.

SysAid made use of incident response services provided by Profero who have discovered that this vulnerability is being actively exploited by Lace Tempest, a group that acts as an affiliate/initial access broker (IAB) for Clop.

LaceTempest has been exploiting the vulnerability to upload a custom webshell, and subsequently launched their malware GraceWire and also Cobalt Strike. The campaign is reported to be fairly complex, with Lace Tempest taking action to cover its tracks and inhibit subsequent investigations.

WithSecure™ Insight

Lace Tempest is a highly capable and sophisticated threat actor and a known affiliate/IAB for the ransomware titan Clop.

The exploitation of SysAid is the fourth known mass-campaign associated with Clop actors this year, which have previously exploited vulnerabilities in GoAnywhere, MOVEit, and PaperCut.

Previous incidents involving Lace Tempest and Clop have occurred at pace and at large scale, impacting hundreds of organizations within a short time scale. If organizations do not remediate this vulnerability, they are likely to be targeted and impacted. Throughout November, Clop posted 11 victims to its leak site. The method behind these compromises is largely unknown.

What can you do?

Thankfully, this vulnerability is limited to on-premises instances of SysAid (<23.3.36), limiting exposure. At the time of writing, there are ~315 SysAid instances exposed to the internet, which are detectable via scanning.

We advise the following:

- Update SysAid to 23.3.36 or greater.
- Conduct a thorough compromise assessment of your SysAid server to look for any known indicators of compromise.
- Review any credentials or other information that would have been available to someone with full access to your SysAid server and check any relevant activity logs for suspicious behavior.

Lazarus' love of supply chains

The North Korean state sponsored APT Lazarus Group has repeatedly used supply chain attacks to compromise victims for both espionage/data theft and financial gain. This month, its most recent supply chain attack was unearthed, in a compromise of CyberLink. In this attack the group compromised the software build process of CyberLink (developers of PowerDVD and other applications), inserting a trojan into its legitimate software installer/updater. When customers downloaded this trusted - yet trojanized - file from CyberLink and executed it, it would perform some system checks, before then downloading second stage payloads, and finally the third stage: malware. This is a very similar attack process to Lazarus Group's compromise of 3CX in Q1 2023, where once again it compromised the software build process and trojanized legitimate software. Fortunately, in both cases it appears that the attacks were detected, and the hosting for the second and third stage payloads was disrupted before the attackers could fully utilize them. The potential scale and impact of such attacks illustrates why DPRK based intrusion sets seem to employ them again and again.

As well as these build process supply chain attacks, in the past Lazarus Group has also targeted software supply chains through poisoned NPM, and PyPi packages - malicious open-source code libraries uploaded to public repositories. The reporting at the time indicated that the packages were most likely intended to target cryptocurrency organizations, but GitHub stated that it believed the group was also targeting the vendors/suppliers used by cryptocurrency organizations.

In Q2/Q3 2023, Lazarus group also compromised the cloud service provider JumpCloud, specifically focusing on the subset of its customers that are cryptocurrency organizations.

WithSecure™ Insight

The different methods of supply chain attack employed by Lazarus group, targeting software build processes, open-source supply chains, and cloud service providers, illustrate several of the non-traditional vectors that determined, capable attackers can employ to compromise not just one victim, but many victims at once through supply chain attacks. Trends in cybersecurity incidents are primarily driven by the success of previous attacks. There are regular innovative attacks which start new trends, but often attackers choose to emulate or iterate upon known successful methods.

As such, it is highly likely that other groups who have the resources to do so will engage in supply chain attacks.

What can you do?

Supply chain attacks are difficult to defend against using traditional security measures because, by definition, they abuse the trust relationship between two entities. However, this does not mean such attacks are impossible to detect or address. The Zero Trust Model is often described as an effective defense against supply chain attacks, as it involves a defense in depth approach where no individual system is trusted, and multiple types of monitoring and protection are put in place to detect abnormal behavior. Behavioral anomaly detection can be a strong defense against supply chain attacks as it makes it possible to look for unusual activity from otherwise trusted users, devices, and processes.

For more information on the growing trend of supply chain attacks, see the WithSecure Supply Chain Threat publication.

2. Hacktivist Landscape

Hamas linked group employ SysJoker malware

Researchers at Check Point have identified a Hamas-affiliated APT group deploying the SysJoker backdoor against entities in Israel.

In December 2021, security experts at Intezer initially uncovered the SysJoker backdoor capable of infecting Windows, MacOS, and Linux systems.

The version utilized in the attacks on Israel is coded in the Rust language, indicating a complete rewrite of the malware. Despite this, the malicious code maintains consistent functionalities with previous iterations. Notably, the threat actor transitioned from Google Drive to OneDrive for storing dynamic C2 (Command and Control) URLs. Intezer has provided an in-depth report on the evolution of SysJoker and its attribution to a group it tracks as WildCard. The backdoor systematically gathers information about the infected system, including Windows version, username, and MAC address. This data is subsequently transmitted to the /api/attach API endpoint on the C2 server.
Check Point also identified behavioral parallels with the Operation Electric Powder campaign, which targeted Israel in 2016-2017. This campaign was attributed to the Gaza Cybergang (aka Molerats), a threat actor with purported ties to the Palestinian organization Hamas.

The Gaza Cybergang exhibits a politically motivated profile and has been operational since at least 2012 and has intensified its activities since then, so it's important to note the group has been active well before the current conflict.

BiBi-Linux Wiper

Research by Security Joes reveals that an anti-Israel hacktivist group, Karma, is likely responsible for attacks utilizing a wiper malware named BiBi-Linux. The malware's name plays on the nickname of Israel's Prime Minister, Benjamin Netanyahu.

In-depth analysis of BiBi-Linux by Security Joes has been published, and ESET researchers have corroborated these findings, identifying a Windows variant of the wiper. This malicious campaign has resulted in the destruction of data at various Israeli organizations, including a data-hosting center and a defense contractor. Notably, the use of a wiper exceeds the typical capabilities associated with hacktivist groups, underscoring Karma as a serious and formidable threat.

While the use of wipers in hacktivist activities is uncommon, Karma exhibits some similarities with another threat actor known as Moses Staff, an Iran-backed group. This connection further emphasizes the significance of Karma's capabilities and the potential geopolitical implications of their actions.

Anonymous Sudan

The group known as Anonymous Sudan has been actively engaged since 2023, and questions surrounding its origins and motives persist. Despite self-identifying as Sudanese hacktivists, compelling evidence suggests their connection to Russian interests.

A comprehensive report by Netscout provides detailed insights into the group's origin and activities, shedding light on its preferred targets. The sectors favored by the group include Airlines, Education, Financial Services, Governmental departments and ministries, Hospitals, and Petroleum distributors.

Notably, Anonymous Sudan has recently declared its utilization of the SkyNet botnet, and is actively promoting access to its DDoS-as-a-service platform on Telegram. This underscores a clear financial motivation behind the group's actions. The group has claimed responsibility for recent attacks on prominent entities such as Netflix, Spotify, OpenAI, and the United Arab Emirates.

Mirai spreading

Akamai has uncovered the exploitation of two zero-day vulnerabilities, reportedly orchestrated to establish a Mirai botnet capable of launching DDoS attacks. In their report, Akamai refrains from naming specific vendors or providing detailed information, citing the ongoing proper disclosure process. However, it reveals that routers and network video recording equipment are implicated, typical targets for botnets.

Mirai, a well-established and widely used botnet variant since 2016, has spawned multiple variants and spin-offs. Typically, access to Mirai botnets is traded for the express purpose of conducting DDoS attacks. The creation and availability of such botnets are increasingly becoming a problematic focus for hacktivist groups, which leverage them as platforms for executing disruptive attacks. This situation poses a growing threat and raises concerns about the potential ramifications of such activities in the cybersecurity landscape.

Water supplies targeted

CISA is responding to incidents involving the compromise of Unitronics Programmable Logic Controllers (PLCs) which are commonly used in the water and wastewater

industry. One such incident involved the compromise of The Municipal Water Authority of Aliquippa in Pennsylvania, USA and Unitronics PLCs are likely the cause behind incidents across the US.

The attacks are being claimed by the Iran-backed group CyberAv3ngers. The group is spreading anti-Israel sentiment and acting in the interests of Iran and Hamas, displaying an ideologically motivated message on compromised equipment.

These compromises are reportedly due to the use of default credentials on PLC systems - a massive oversight - as well as a reminder that security is multi-layered and replacing default credentials with hardened ones is vital in all environments, but especially within critical national infrastructure on which millions of people rely. It also serves as a reminder that geopolitically motivated attackers and hacktivist groups can and do target organizations and individuals operating outside of the immediate geographical and industrial sphere.

Indian Cyber Army

The Indian hacktivist group Indian Cyber Army have begun a campaign directed at Qatari organizations and entities; these attacks are in response to the Qatar courts sentencing 8 Indian Navy officers to death following their trial in relation to alleged espionage.

The Indian Cyber Army are a capable group who engage in DDoS, website defacements and breach exposed and vulnerable networks and systems, including CCTV. The group actively promote their activity on X and Telegram and are also actively targeting Pakistan and China. Any geopolitical event in opposition to the interests of India is likely to place the opposing nation within scope of Indian Cyber Army attacks.

3. Ransomware: Trends and Notable Reports

The following data is limited to ransomware and data leak groups who operate a leak site which is parseable. The following data was captured between 1st November – 30th November 2023.

Overall there has been a 25% increase in activity compared to October, which in reality is a return to “normal” figures (taken from a 2021 and 2022 benchmark), as October had seen a sharp -28% fall.

Just one newcomer this month in the form of Meow, another group using Conti source-code, which we discuss in more detail below.

In addition to our monthly Threat Highlight Report, WithSecure has recently published a report that focuses on ransomware in 2023, and the impact of newcomers to the landscape, including examination of how many of these groups are truly novel. The research is available here.

LockBit’s CitrixBleed Campaign

In last month’s Threat Highlight Report, we highlighted the danger associated with CVE-2023-4966 “Citrix Bleed”, a vulnerability in Citrix NetScaler ADC and Gateway which has allowed attackers to steal session cookies/tokens and therefore gain initial access into networks.

This access has subsequently been abused by ransomware groups/affiliates to launch attacks, most notably LockBit.

LockBit published 112 victims on its leak site in November, making it the group’s busiest month since August, and its fourth busiest month this year so far. There is no doubt that many of those cases are due to the group’s exploitation of Citrix Bleed.

Many of LockBit’s attacks have been highly impactful, and carried out at scale and at pace, suggesting a concerted and professionalized effort. This further demonstrates that LockBit is a highly capable and very well-resourced organized crime group.

Group	Victims	Percentage	Change from last month
3am	3	1	5
8Base	33	7	65
Abyss Data	4	1	300
Akira	19	4	58
Alphv (BlackCat)	52	10	58
BianLian	13	3	-7
BlackBasta	41	8	128
Black Suit	7	1	250
Cactus	10	2	100
CiphBit	2	0	Returned
Clop	11	2	Returned
Cuba	4	1	33
Daixin	2	0	Returned
Donut Leaks	4	1	33
Everest	1	0	No Change
Hunters International	17	3	750
INC Ransom	15	3	67
Knight	6	1	No Change
LockBit	112	22	78
Lorenz	4	1	100
Medusa	14	3	-26
Meow	9	2	Newcomer
MetaEncryptor	2	0	Returned
Monti	5	1	-38
NoEscape	24	5	-63
Play	44	9	10
Qilin	5	1	No Change
RA Group	9	2	Returned
RansomExx	2	0	100
Ransomhouse	3	1	33
Ransomware Blog	2	0	-33
Rhysida	12	2	140
Snatch	10	2	100
Total	501		25

Public reporting has linked the high-profile attacks on ICBC, Boeing, DP World, Allen & Avery and many others to the exploitation of Citrix Bleed.

While Citrix released patches for Citrix Bleed back in October, it appears that in-the-wild compromise was already underway, and the vulnerability continued to be successfully exploited due to a lack of prompt patch management and failure to purge stolen session tokens.

Alphv's new tactics

Malicious advertising (malvertising) and SEO poisoning are malware distribution methods we have discussed frequently throughout 2023 and highlighted as a consistent problem and tactic utilized by all types of threat actors.

Reporting by eSentire, Securonix, and Trend Micro this month has reinforced this trend, and has specifically highlighted an ongoing malware distribution campaign by affiliates of the ransomware group Alphv (BlackCat).

Alphv is a highly capable and well-resourced ransomware group whose affiliates typically rely upon the use of valid credentials gained via initial access brokers in order to gain access, and now also utilize malvertising. Alphv is pushing fake advertising for popular software such as Advanced IP Scanner, WinSCP, Cisco AnyConnect and Slack, with the ultimate goal of infecting victims with Nitrogen, an initial access malware.

If one new tactic wasn't enough, Alphv has also introduced another far more unusual tactic to their repertoire: reporting companies to the authorities.

DataBreaches.net reported on this bizarre situation, in which an Alphv affiliate submitted a report to the US Securities and Exchange Commission (SEC) reporting that one of its victims had failed to properly declare a breach, applying pressure on the victim and alerting third parties to the incident. At the time of writing, this is the only know case involving this type of extortion, and whether it will be further adopted remains to be seen.

Yanfeng automotive targeted

The Chinese automotive interior component supplier Yanfeng has been struck by the Qilin ransomware group. Yanfeng are a supplier for General Motors, the Volkswagen Group, Ford, Stellantis, BMW, Daimler AG, Toyota, Honda, Nissan, and SAIC Motor. The attack reportedly caused issues for some car makers, ultimately leading to manufacturing delays, so it's not just cyber supply chains that are complex and problematic!

Qilin was inactive between November 2022 and March 2023, but has since been a consistent threat. On average the group posts five victims to its leak site each month. This attack follows a recent trend of Chinese organizations being targeted, and while only five Chinese entities have been publicly impacted over the last 90 days, this still pales in comparison to the USA (578), UK (84) or Australia (24). Regardless, it is certainly a shift, as China is rarely targeted.

Energy Sector under fire

Slovenia's largest energy supplier Holding Slovenske Elektrarne (HSE) has experienced a ransomware attack which left some systems and files encrypted. The organization has approached the situation with absolute transparency, stating it is yet to receive any ransom demands, and is also working in cooperation with the Slovenian National Office for Cyber Incidents and Law Enforcement.

This attack did not cause any disruption to services or impact customers, but follows a worrying trend of the energy sector being targeted by threat actors. The much-publicized cyber attacks on critical national infrastructure within Ukraine orchestrated by Sandworm (Russia's GRU) are a worst-case example of this, but both financially motivated and state-backed groups are also seeking to breach energy firms on an almost constant basis.

Hunters International

Newcomers Hunters International burst onto the scene in late October, and there were indicators that the group were a spin-off group of the defunct Hive group, famously shut down in January 2023 by a joint law enforcement operation. In response to this speculation, Hunters International has made a statement saying it is not a rebrand of Hive, but it has actually acquired the group's source code as part of a deal during Hive' demise, and are in fact an independent gang. This is believable, as the connection between Hive and Hunters International was based on code overlap. However, this may also be an effort by the group to distance itself from its origins and the Hive name due to way in which they were targeted by law enforcement, not wishing to attract the same attention.

Stop right Meow!

A newcomer for November is ransomware group Meow, which dumped data relating to nine different victims on its dark web leak site within two days. Some IOCs associated with the group have been shared online, and Meow joins a long and growing list of groups that are recycling Conti's leaked source code.

At the time of writing, Meow's victims originate from various sectors, and are based in the USA, Morocco and Nigeria. Entities within African nations are not normally popular targets for ransomware groups, but assessment as to whether this is a trend or just opportunistic behavior relies on more data: one to watch!

Qlik Sense gets prickled

Analysis by Arctic Wolf has identified a campaign by Cactus to exploit vulnerabilities in Qlik Sense in order to launch ransomware attacks. The report states that "Qlik Sense is likely being exploited either via the combination or direct abuse of CVE-2023-41266, CVE-2023-41265 or potentially CVE-2023-48365 to achieve code execution".

In these incidents the hackers abused the Qlik Sense scheduler service to spawn other processes, including downloading a payload from an attacker-controlled website. This campaign is of particular interest as Qlik released fixes in August, but Cactus was able to create bypasses and continue to exploit the vulnerability, resulting in the need for another patch, which has since been issued.

Ardent Health experiences real world impact

The real-world impact of cyber-attacks is something we often highlight, as we seek to reinforce the absolute need for security and best practices, because the impacts can be severe and far-reaching. Yet another example of this is a recent ransomware attack on Ardent Health Services, who are responsible for 30 different hospitals across six US states. While Ardent appear to have handled the incident well and with transparency, some procedures have had to be cancelled and services diverted, thankfully this has not caused major issues, but is a stark reminder of how bad a ransomware attack can really be.

4. Other notable highlights in brief

SolarWinds lawsuit

Since the SolarWinds supply chain attacks of December 2020, there has been constant speculation as to the root cause of the compromise, with an intern being (wrongly) blamed, and rumors of a lackadaisical security culture.

A clearer picture appears to be getting painted as the SEC has filed a lawsuit against SolarWinds and its CISO, Timothy Brown, alleging the defendant's' attitude and behaviors led to poor cyber security practices, with the first section of the lawsuit stating:

"From at least October 2018 through at least January 12, 2021, defendants SolarWinds and its then-Vice President of Security and Architecture, Brown, defrauded SolarWinds' investors and customers through misstatements, omissions, and schemes that concealed both the Company's poor cybersecurity practices and its heightened and increasing cybersecurity risks. SolarWinds' public statements about its cybersecurity practices and risks painted a starkly different picture from internal discussions and assessments about the Company's cybersecurity policy violations, vulnerabilities, and cyberattacks".

In episode #84 of WithSecure's podcast "Cyber Security Sauna", analysts Ziggy Davies and Stephen Robinson discussed the importance of transparency when it comes to security and incidents. Unfortunately, in the case of SolarWinds it appears the exact opposite has occurred, and staff actively misled others about the state of security at the company, and on at least one occasion are alleged to have directly lied about the cause of an incident.

This lawsuit may well set a precedent for holding companies and their employees directly responsible for the shortcomings of their security, which will hopefully have the impact of promoting a proactive and transparent approach to security.

Okta update

In October's edition of the Threat Highlight Report we discussed the compromise of Okta which led to further compromises at some of its customers. At the time Okta stated that due to the compromise of the company's customer support system, about 1% of its customers had been impacted. Okta has since made a further statement saying that all the users of its customer support system have been impacted. Thankfully the impact for these customers is not as severe as last month's announcement, with the exposure being limited to PII such as full name and email addresses.

The leaking of PII has potentially harmful consequences including becoming a target for phishing and social engineering attacks, we advise being on guard for such attacks, as well as reviewing your password and MFA settings and policies.

Scarred Manticore

Check Point Research (CPR) has been actively monitoring an ongoing Iranian espionage campaign orchestrated by Scarred Manticore, an actor with affiliations to the Ministry of Intelligence and Security (MOIS). The campaign, which peaked in mid-2023, remained undetected for at least a year and specifically targets high-profile organizations in the Middle East. The focus extends to government, military, and telecommunications sectors, as well as IT service providers, financial organizations, and NGOs.

Scarred Manticore employs an advanced malware framework called LIONTAIL, installed on Windows servers. To

enhance stealth, LIONTAIL implants utilize direct calls to the Windows HTTP stack driver HTTP.sys, loading memory-resident payloads. Collaborating with Sygnia's Incident Response team, CPR utilized various forensics tools and techniques to unveil additional stages of the intrusions and the intricacies of the LIONTAIL framework. Although the primary motivation behind Scarred Manticore's operations is espionage, it's noteworthy that some tools associated with the campaign have also been linked to MOIS-sponsored destructive attacks, such as the one against Albanian government infrastructure known as DEV-0861.

Blaze Stealer

Throughout 2023, another significant supply chain threat has emerged as attackers distributed malicious Python packages, masquerading as legitimate tools on common repositories. One example examined by Checkmarx is named "BlazeStealer," and upon activating its malicious payload, it fetches an additional harmful script from an external source. The outcome of this attack is the deployment of a Discord bot, granting attackers comprehensive control over the victim's computer.

Particularly vulnerable to this threat are developers engaged in code obfuscation, as they often handle valuable and sensitive information. This makes them prime targets for hackers seeking unauthorized access, emphasizing the strategic targeting of victims in this campaign.

Atomic Stealer

Atomic Stealer, or AMOS, has established itself as a prominent threat to MacOS users. In a recent development observed in September, the malware adopted a deceptive approach, exploiting malicious ads to dupe unsuspecting victims into downloading it disguised as a popular application.

In a noteworthy shift, AMOS has taken a new delivery route to Mac users, leveraging a deceptive browser update chain identified as 'ClearFake.' This marks a significant departure from previous techniques used by the group, as attackers traditionally focus on Windows platforms in social engineering campaigns.

The Australian approach

Australia has experienced a particularly tough few years when it comes to cyber security, with highly impactful incidents involving Optus, and more recently DP World, both of which had real world repercussions for Australians. In response to this deluge, Australia has announced a new cyber strategy covering the years 2023-2030, which is set to cost $587 (AUD) million.

One of the biggest elements of the plan is greater protections and services for small and medium businesses, for whom cyber-attacks can often be fatal. Plans for these businesses include free cyber health assessments and resources to train staff on common dangers. Other areas focus on greater joint working and cooperation, as well as a clear focus on enabling transparency.

5. Threat data highlights | Vulnerabilities & Exploits

Citrix Bleed
CVE-2023-4966

As discussed above in the “LockBit’s CitrixBleed campaign” section, this vulnerability has been heavily targeted by ransomware groups, and has resulted in many highly impactful incidents.

Atlassian Confluence
CVE-2023-22518

Atlassian describes the vulnerability as an “Improper Authorization Vulnerability in Confluence Data Center and Confluence Server” and we are aware that it is being actively targeted by threat actors including ransomware groups.

Apache Active MQ
CVE-2023-46604

Open source reporting indicates that this vulnerability is being actively targeted by ransomware groups including HelloKitty.

F5 BIG-IP
CVE-2023-46747

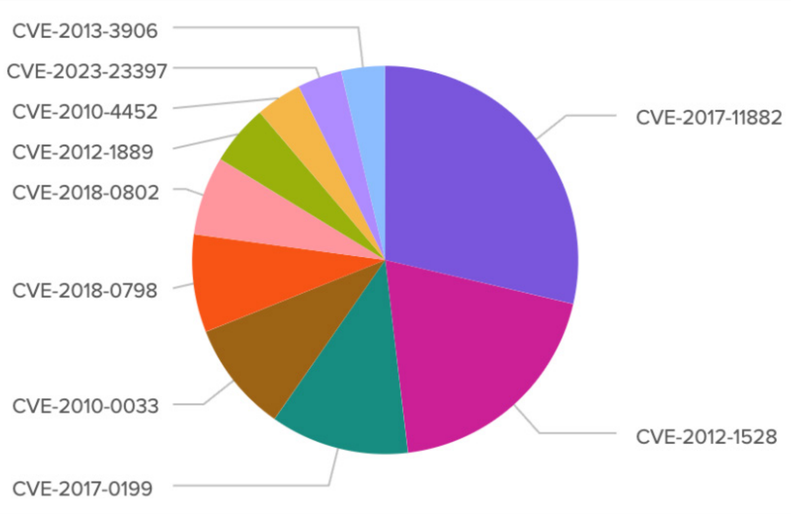
Threat actors are exploiting CVE-2023-46747 together with CVE-2023-46748 as part of an exploit chain in observed attacks in the wild. Patches are available to fix this issue, and F5 have released relevant advice.

WinRAR
CVE-2023-38831

This vulnerability has escalated and been targeted by numerous threat actors since April 2023. In a recent campaign it is alleged that Russia is using the vulnerability to target Azerbaijan, Greece, Romania and Italy for the purposes of espionage.

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



What vulnerabilities are being newly exploited?

CVE ID	Vendor / Product	CVSS Rating	What's the vulnerability?
CVE-2023-46604	Apache ActiveMQ	CRITICAL	Apache ActiveMQ contains a deserialization of untrusted data vulnerability that may allow a remote attacker with network access to a broker to run shell commands by manipulating serialized class types in the OpenWire protocol to cause the broker to instantiate any class on the classpath.

The following are additions to CISA's known exploited vulnerability catalog in November. 7 have received "CRITICAL" CVSS ratings.

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