Threat Highlight Report

July 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 exploitation of Ivanti EPMM (MobileIron) resulting in the compromise of government departments in Norway, probably by a state-backed sophisticated threat actor. We also discuss driver loopholes, the exploitation of Citrix products, a TeamsPhisher tool that is being ignored by Microsoft, and examine the hacktivist landscape.

This month's ransomware landscape includes an incident involving newcomers BigHead, as well as coverage on the impersonation of Sophos, the use of malvertising, and a 2-for-1 incident at cosmetics brand Estée Lauder. As always, we also include statistics relating to the most active groups throughout July.

- Ziggy Davies, Intelligence Analyst

1 Monthly highlights

1.1 Norway uncovers MobileIron breach

A critical vulnerability in a mobile device management service by Ivanti called Endpoint Manager Mobile (EPMM) (formerly known as MobileIron) (CVE-2023-35078), has earned a rare CVSS score of 10.0 and is confirmed to be the cause of breaches within the Norwegian government.

Ivanti has published a security advisory and released a patch which fixes the issue, but not before at least 10 organizations had been breached by an unknown threat actor. The Norwegian Government and Security Service (DSS) has stated that the vulnerability has been exploited by an unknown threat actor, in order to compromise 12 ministries.

The vulnerability has been described as an API access vulnerability, suggesting the default (from Ivanti documentation) URI path `https://[core server]/vulnerable-path/api/v2` was able to be used by an unauthenticated attacker to execute commands. A second vulnerability was also exploited to achieve Remote Code Execution, and, at the time of writing, detailsare not public. The authentication bypass is trivial to exploit and once a public exploit is made available, it will almost certainly be exploited by opportunistic threat actors.

WithSecure™ Insight

Successful attacks on Mobile Device Managers can be disastrous for organizations, as they acts as high privilege hubs for all mobile devices through which it is possible to access a wealth of sensitive organizational data and communications.

Any information available on EPMM's MIFS portal should be considered to be available to a successful attacker. Device management functions are also available to attackers (policies, pushed applications etc.). Device information, geolocation, and user information should also be considered available to an attacker.

At the time of writing, the exploitation of this vulnerability has not been attributed to any specific threat actor or nation-state. While Norway has previously been attacked by Russian-backed groups such as **KillNet**, and recent geopolitical news will have likely piqued the interest of China, any attempt at attribution without further information about the technical aspect of the compromises would be pure speculation.

What can you do?

This vulnerability is present in all versions of EPPM from 11.10 and earlier, and must be patched to the latest version. If you are unable to patch, Ivanti have provided mitigation advice within their customer knowledge base.

1.2 Driver loopholes

Starting with Windows 10 version 1607, Microsoft has updated its driver signing policy to no longer allow new kernel-mode drivers that have not been submitted to and signed by its Developer Portal. In order to maintain the functionality and compatibility of older drivers on devices with certain OS configurations, Microsoft created certain exceptions to this policy. These exceptions can be exploited by threat actors to load malicious drivers that would otherwise be blocked, with several open-source tools available to aid the process.

The loophole that is being exploited allows threat actors to load malicious kernel-mode drivers with expired certificates. This is done by forging the signature timestamp on a driver, making it appear as if it was signed before the policy change. This allows them to load malicious drivers that would otherwise be blocked by Windows.

Research by Talos has found multiple open-source tools designed to forge pre-2015 certificates into malicious drivers, so that they can be run.

The tools discussed are:

- HookSignTool (GitHub)
- F*ckCertVerifyTimeValidity (GitHub)

WithSecure™ Insight

This technique appears to be largely used by Chinese language threat actors, as seen in a recent campaign called RedDriver**.** This technique is used to sign a malicious driver, which is then used to steal browser traffic and is being heavily discussed on Chinese language hacking forums.

While this technique is commonly used to achieve somewhat benign means (to an enterprise), such as the signing of game cheats, etc., the **RedDriver** campaign is an example of how this technique can be used to deploy malware in environments in which it should ordinarily be blocked.

It is not outside the realms of possibility that the technique could be chained into BYOVD or similar malicious activity to bypass revoked or blocked certificates.

What can you do?

This technique is designed to bypass restrictions that have been enforced since Windows 10 version 1607. The best way to protect against this technique is by using security solutions such as AV and EPP/EDR. WithSecure™ has been developing capabilities in our products to detect the abuse of vulnerable drivers, to align with the on-going trend amongst adversaries. Currently, we have many detection capabilities in production that, for example, monitor driver loading. We will continue this development, and are paying close attention to novel methods that abuse device drivers as they emerge.

1.3 Citrix Exploitation

This month there has been active exploitation of two new vulnerabilities in two different Citrix products, namely ShareFile and NetScaler (ADC).

ShareFile, a file sharing application offered by Citrix has come under attack following the reporting of a Remote Code Execution (RCE) vulnerability (CVE-2023-24489) in the application's storage zone controller function.

Likewise, Citrix NetScaler (ADC) is also being targeted via another RCE vulnerability (CVE-2023-3519), as well as two others mentioned in a security bulletin by Citrix.

It is highly likely that both vulnerabilities were being exploited as a zero day, but the products now have patches made available by Citrix.

WithSecure™ Insight

Unpatched Citrix ADC server exploitation is a common intrusion vector for a plethora of cyber-criminal gangs, and, in keeping with this, the new vulnerability remains under exploitation by a wide spectrum of threat actors. Organizations vulnerable to this should ensure that they patch as soon as possible, while threat hunters should be aware of this vulnerability and the likelihood that it will be targeted, watching for the presence of web shells and erroneous or atypical behavior.

The exploitation of ShareFile is the latest in a long list of file transfer applications to be targeted by threat actors. It is highly likely that the exploitation is being undertaken by financially motivated threat actors, probably operating out of Eastern Europe and Russia.

The compromise of file transfer applications such as this and MOVEit aligns with other attacks by ransomware actors, such as the attacks on GoAnywhere MFT and Accellion File Transfer Appliance (FTA). Ransomware actors are actively developing zero-day exploits for prevalent enterprise software, with the intention of striking large numbers of organizations within a rapid timeframe. With extortion-only ransomware on the rise, targeting file transfer services has become commonplace.

Ransomware actors who have targeted file transfer systems historically include: **Buhit, IceFire** and **Clop.**

WithSecure™ has detected instances of ShareFile which may be vulnerable, and a search on Censys with the following recipe detects 1,311 hosts on the Internet (at the time of writing), with the majority being in the United States:

```
(services.http.response.html_tags="<title>ShareFile: Securely Sync, Store and Share Files</title>")
```

Or

```
(services.http.response.html_tags="<title>ShareFile Storage Server</title>")
```

What can you do?

Customers with self-controlled ShareFile instances (<5.11.24) are advised to update to the newest version.

Customers using Citrix NetScaler are advised to update to the follow versions of products:

- NetScaler ADC and NetScaler Gateway 13.1-49.13 and later releases
- NetScaler ADC and NetScaler Gateway 13.0-91.13 and later releases of 13.0
- NetScaler ADC 13.1-FIPS 13.1-37.159 and later releases of 13.1-FIPS
- NetScaler ADC 12.1-FIPS 12.1-65.36 and later releases of 12.1-FIPS
- NetScaler ADC 12.1-NDcPP 12.1-65.36 and later releases of 12.1-NDcPP

1.4 Microsoft ignores TeamsPhisher

The default configuration of Microsoft Teams deployments allows external users to message internal users. But when they do, messages from external users are marked as external, and they will not be able to send files. This mitigates the risk of malware ingressing into a network via Teams, a vector that some may struggle to monitor, particularly without incurring additional cost.

Researchers have discovered that these security controls are implemented in the client, not the server. As such, by editing the HTTP POST request to swap the internal recipient ID and the external sender ID, the message is not flagged as internal, and sent files are received by the recipient as if they were from a trusted internal sender.

The TeamsPhisher tool is a python script which not only automates the process of exploiting this vulnerability to send a message, but accepts a list of users to target, a message text, and a payload file.

Unfortunately, Microsoft have dismissed the issue and apparently do not have any plans to address the vulnerability.

WithSecure™ Insight

Microsoft Teams is an almost ubiquitous enterprise collaboration platform, and many users in a large enterprise will trust that a message received via Teams which is not marked as internal, in contradiction to how they would normally treat contact from an unknown source.

The researchers behind **TeamsPhisher** have demonstrated that this issue can be used to phish a victim very easily and simply during a live red-team engagement. As they point out, phishing protections for email do not apply to Microsoft teams, so reputation, domain age, etc., are not considered. An attacker can simply register a similar domain and use it straight away in an attack.

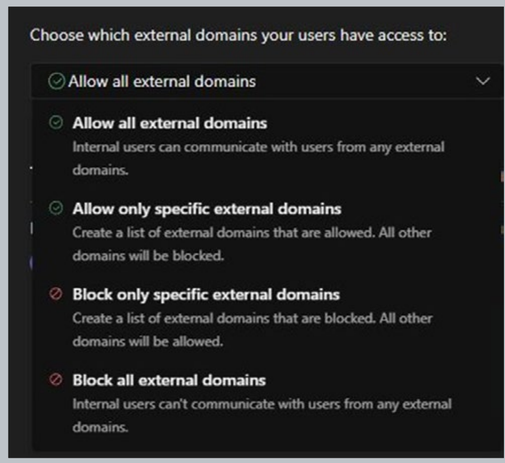
The **TeamsPhisher** tool will enable attackers with very basic technical skills, who may not otherwise have been able to exploit this vulnerability, to use it in phishing campaigns against organizations which use Microsoft Teams. As such, it is likely that the targeting of this vulnerability will increase.

Microsoft's dismissal of this vulnerability is frustrating and perhaps highlights the issue of where a single organization is responsible for intended functionality and security, and therefore has to prioritize one over the other.

What can you do?

The default configuration of Microsoft Teams means that external contacts can message members of the organization, making them vulnerable to the use of **TeamsPhisher.** It is possible to block this behavior by changing to 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.



1.5 Hacktivism

CyberAnarchySquad

The pro-Ukraine hacktivist group **CyberAnarchySquad** have attacked and disrupted the services of Russian satellite Internet provider Dozortel.

IT Army of Ukraine

Ukraine's official volunteer hacktivist group, the **IT Army of Ukraine,** has successfully targeted and disrupted the services of Russian railway company RZD, leading to the website and application being unavailable for 6 hours.

NoName057(16)

The pro-Russian hacktivist group **NoName057(16),** which runs the DDoSIA project, has continued its DDoS campaign by heavily targeting organizations in Italy, Spain, New Zealand, the UK, Austria, Lithuania, France and Norway.

2 Ransomware: Trends and notable reports

The following data is limited to a multi-point of extortion ransomware leak sites that are parseable and captured between 29th June, 2023 and 27th July, 2023. Overall, there has been a small (+8%) increase in activity during July. Despite 8 of the top groups experiencing a reduction in activity, the boost is attributable to the massive number of victims posted by **Clop** in relation to their exploitation of MOVEit. Newcomers **Cactus** and **Cyclops** are also responsible for 24 victims between them.

Group	Victims	Percentage	Change
Clop	183	39%	135%
LockBit	46	10%	-23%
8Base	35	7%	-10%
Alphv	29	6%	-24%
Play	24	5%	-29%
Cactus	18	4%	New
Akira	15	3%	-38%
Rhysida	15	3%	-12%
Bianlian	14	3%	0%
BlackBasta	13	3%	-55%
NoEscape	11	2%	57%
Medusa	10	2%	-41%
Stormous	8	2%	800%
Cyclops	6	1%	New
Other	41	N/A	N/A
Total	**468**		**8%**

2.1 BigHead ransomware

This month the WithSecure™ Incident Response team attended a ransomware incident perpetrated, as claimed in the ransom note, by a group called ‘DEADbyDAWN’. The encryptor used appears to be **BigHead** ransomware, a relatively new variant observed in the wild. **BigHead** ransomware actors have been observed compromising victims through malvertising and fake Windows updates.

In this campaign, the DeadByDawn team likely employed legitimate credentials to authenticate the VPN. TTPs echo typical ransomware infections with AnyDesk, Cobalt Strike, Advanced IP Scanner and RDP connections. The threat actor threatened to publish stolen data and leverage the media to damage the reputation of the victim.

2.2 8Base connected to RansomHouse?

The ransomware group **8Base** burst onto the scene in May 2023 with a surge of posts on their dark web leak site, and, at time of writing, have published data relating to at least 142 victims. Recent analysis has shown striking similarities in the verbiage used by **8Base** and **RansomHouse,** a group who have been active since May 2022. It appears 8Base have copied the language and formatting used on the following: ransom note, leak site content, terms of service and FAQ.

This presents a few questions: are **8Base** and **RansomHouse** connected in some way? Have **8Base** simply copied some content from **RansomHouse?**

2.3 2-for-1 at Estée Lauder

Cosmetics brand Estée Lauder have had a difficult month, declaring a cyber incident which has been claimed by both the ransomware group **Alphv** (BlackCat) and **Clop.** The compromise by **Clop** is part of their MOVEit exploitation, with Estée Lauder joining over 250 other organizations listed on **Clop’s** leak site so far. Meanwhile, **Alphv** have taunted the cosmetic brand, claiming to still have access to the network and stolen data. Interestingly, **Alphv** have not encrypted any data, and appear to have shifted to a data theft and extortion tactic on this occasion.

2.4 Ransomware group impersonates Sophos

A sample of ransomware uploaded to ID Ransomware and VirusTotal has been analyzed and shown to include elements which impersonate the branding and name of the cybersecurity company.

Sophos investigated the matter and believe this to be a simple case of brand impersonation, something which is not that uncommon. The ransomware itself is described by Sophos as “closer to a general-purpose remote access trojan (RAT) with the capability to encrypt files”, something that is unusual for modern ransomware malware, which are normally bespoke lockers. At the time of writing, there does not appear to be a wider campaign using the malware, with only a few samples appearing online.

2.5 Malvertising used by Alphv

Malvertising is a common way to distribute malware, with advertising services like Google Ads being an easy way for threat actors to boost the interaction of unwitting victims with their malicious websites. A recent incident has shown that a malvertising campaign targeting users looking for the legitimate program **WinSCP,** has ultimately resulted in compromise by a threat actor with overlapping TTPs associated with the ransomware group **Alphv** - and, in one instance, the detonation of **Alphv's** locker.

Malvertising is a dangerous initial access vector, with many users understandably believing they can trust the top links on a Google search, without realizing they are paid adverts which are not vetted by Google. In many cases, malicious websites perfectly mimic legitimate services and are hard to detect. It is therefore vital that organizations raise awareness around the risk of malvertising and SEO poisoning, helping users identify risks and avoid compromise, while also making use of security solutions such as AV and EPP/EDR.

2.6 Ransomware Newcomers

Cactus

This group has been busy, posting relating to 18 victims during July Analysis suggests that they are exploiting vulnerable VPN instances to gain initial access. The TTPs used by Cactus follow a standard ransomware playbook, making use of well-known tooling.

3 Other notable highlights in brief

3.1 CISA warns of an increase in Truebot activity

An advisory published by CISA has warned about an increase in **Truebot** activity across the US and Canada. While **Truebot** has traditionally been delivered via phishing, the advisory warns that the group behind the malware has begun distributing it following the exploitation of a vulnerability in Netwrix Auditor (CVE-2022-31199).

Truebot is associated the with group behind **Clop,** which has recently made headlines following their exploitation of MOVEit. They have also used it to gain initial access and deploy other malware variants in their arsenal, such as **FlawedGrace** and **Cobalt Strike.**

3.2 RomCom targets NATO summit guests

A recent campaign targeting guests at the recent NATO summit in Lithuania has been attributed to a threat actor called **RomCom.**

In this campaign, the threat actor delivered weaponized MS Word documents which were contained within a well-crafted replica of the NATO summit website. The analysis by BlackBerry states:

“Based on the nature of the upcoming NATO Summit and the related lure documents sent out by the threat actor, the intended victims are representatives of Ukraine, foreign organizations, and individuals supporting Ukraine”.

3.3 Attempted JumpCloud supply chain attack

A recent attack investigated by Mandiant has been attributed to the DPRK-backed group **TraderTraitor,** a sub-group of the nation’s **Reconnaissance General Bureau** (RGB). The campaign began with a sophisticated spear phishing campaign aimed at JumpCloud, which is a zero-trust directory platform used for identity and access management, with the end goal being the compromise of JumpCloud users from the blockchain/crypto sector. This type of downstream chain supply attack is becoming a popular tactic amongst sophisticated threat actors, with the compromise of X_Trader and 3CX applications prevalent.

Attribution has been aided in this case thanks to an operational security failure by an **RGB** member, who connected to attack infrastructure directly from a DPRK IP address. This failure is like one WithSecure™ witnessed during the recent No Pineapple! investigation. Perhaps some OpSec training is in order.

3.4 OSS supply chain attacks target the banking sector

A recent investigation into malicious open source software (OSS) packages has uncovered two different campaigns targeting banks. In both instances, popular repositories were tainted with malicious code in the style of supply chain attack that is becoming increasingly popular.

The attacks were targeted using malicious code designed to exploit specific web assets from each bank.Both threat actors appear to be sophisticated, using social engineering and advanced techniques to remain undetected.

In the first attack the end goal was unclear, with the attackers being detected following their usage of the open-source post exploitation command and control framework Havoc. The second attack was more clear-cut, with the attackers modifying code on the banks' user login page in an attempt to steal credentials, suggesting a financially motivated actor.

4 Threat data highlights

4.1 Vulnerabilities & Exploits

What is everyone talking about?

The following are the vulnerabilities which have been heavily discussed on social media in June.

1. CVE-2023-35078
   Ivanti Endpoint Manager Mobile (MobileIron)
   The exploitation of EPMM tops the list this month, with the compromise of several Norwegian government ministries in a likely state-backed targeted attack being a hot topic for the cyber community and general news agencies alike.

2. CVE-2023-38408
   OpenSSH
   This RCE vulnerability exists due to an incomplete fix of an older 2016 vulnerability, and is present in most Ubuntu instances. It also requires a patch.

3. CVE-2023-24489 & CVE-2023-3519
   Citrix ShareFile & Citrix NetScaler (ADC)
   As previously discussed, both of these vulnerabilities are being actively exploited by financially motivated threat actors. ShareFile presents an alluring entry point for data theft, while NetScaler would be an ideal initial access vector for further compromise. Patches for both are available from Citrix.

What have we seen?

The attempted exploitation of CVE-2023-21716 is increasing in prevalence, with a 363% spike in our telemetry since last month. This vulnerability is present in outdated Microsoft Word instances and can be abused by attackers delivering a specially crafted Rich Text File (.rtf), which can result in the execution of malicious code.

What vulnerabilities are being newly exploited?

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

CVE-10	Vendor / Product	CVSS Rating	What's the vulnerability?
CVE-2023-35078	Ivanti Endpoint Manager Mobile (EPMM, fka MobileIron)	Critical (10}	Ivanti Endpoint Manager Mobile (EPMM, previously branded MobileIron Core) contains an authentication bypass vulnerability that allows unauthenticated access to specific API paths. An attacker with access to these API paths can access personally identifiable information (PU) such as names, phone numbers, and other mobile device details for users on a vulnerable system. An attacker can also make other configuration changes, including creating an EPMM administrative account that can make further changes to a vulnerable system.
CVE-2022-31199	Netwrix Auditor	Critical	Netwrix Auditor User Activity Video Recording component contains an insecure objection deserialization vulnerability that allows an unauthenticated, remote attacker to execute code as the NT AUTHORITY\SYSTEM user. Successful exploitation requires that the attacker is able to reach port 9004/TCP, which is commonly blocked by standard enterprise firewalling.
CVE-2022-29303	SolarView Compact	Critical	SolarView Compact contains a command injection vulnerability due to improper validation of input values on the send test mail console of the product's web server.
CVE-2023-3519	Otrix NetScaler ADC/Gateway	Critical	Citrix NetScaler ADC and NetScaler Gateway contains a code injection vulnerability that allows for unauthenticated remote code execution.
CVE-2021-29256	Arm Mali GPU	High	Arm Mali GPU Kernel Driver contains a use-after-free vulnerability that may allow a non-privileged user to gain root privilege and/or disclose information.
CVE-2023-32046	Microsoft Windows	High	Microsoft Windows MSHTML Platform contains an unspecified vulnerability that allows for privilege escalation.
CVE-2023-32049	Microsoft Windows	High	Microsoft Windows Defender SmartScreen contains a security feature bypass vulnerability that allows an attacker to bypass the Open File - Security Warning prompt.
CVE-2023-35311	Microsoft Outlook	High	Microsoft Outlook contains a security feature bypass vulnerability that allows an attacker to bypass the Microsoft Outlook Security Notice prompt.
CVE-2023-36874	Microsoft Windows	High	Microsoft Windows Error Reporting Service contains an unspecified vulnerability that allows for privilege escalation.
CVE-2023-36884	Microsoft Windows/Office	High	Microsoft Office and Windows contain an unspecified vulnerability that allows an attacker to perform remote code execution via a specially crafted Microsoft Office document.
CVE-2023-29298	Adobe ColdFusion	High	Adobe ColdFusion contains an improper access control vulnerability that allows for a security feature bypass.
CVE-2023-37450	Apple	Under Review	Apple iOS, iPadOS, macOS, and Safari WebKit contain an unspecified vulnerability that can allow an attacker to execute code when processing web content.
CVE-2023-38205	Adobe ColdFusion	Under Review	Adobe ColdFusion contains an improper access control vulnerability that allows for a security feature bypass.
CVE-2023-38606	Apple	Under Review	Apple iOS, iPadOS, macOS, tvOS, and watchOS contain an unspecified vulnerability allowing an app to modify a sensitive kernel state.
CVE-2023-37580	Zim bra Collaboration	Under Review	Zimbra Collaboration Suite (ZCS) contains a cross-site scripting vulnerability impacting the confidentiality and integrity of data.
CVE-2023-35081	Ivanti Endpoint Manager Mobile (EPMM, fka MobileIron)	Under Review	Ivanti Endpoint Manager Mobile (EPMM) contains a path traversal vulnerability that enables an authenticated administrator to perform malicious file writes to the EPMM server. This vulnerability can be used in conjunction with CVE-2023-35078, bypassing administrator authentication and ACLs restrictions (if applicable).

About WithSecure™

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