CYFIRMA

DECODING THREATS

CRITICAL EXPLOITS FOR SALE ON THE DARK WEB

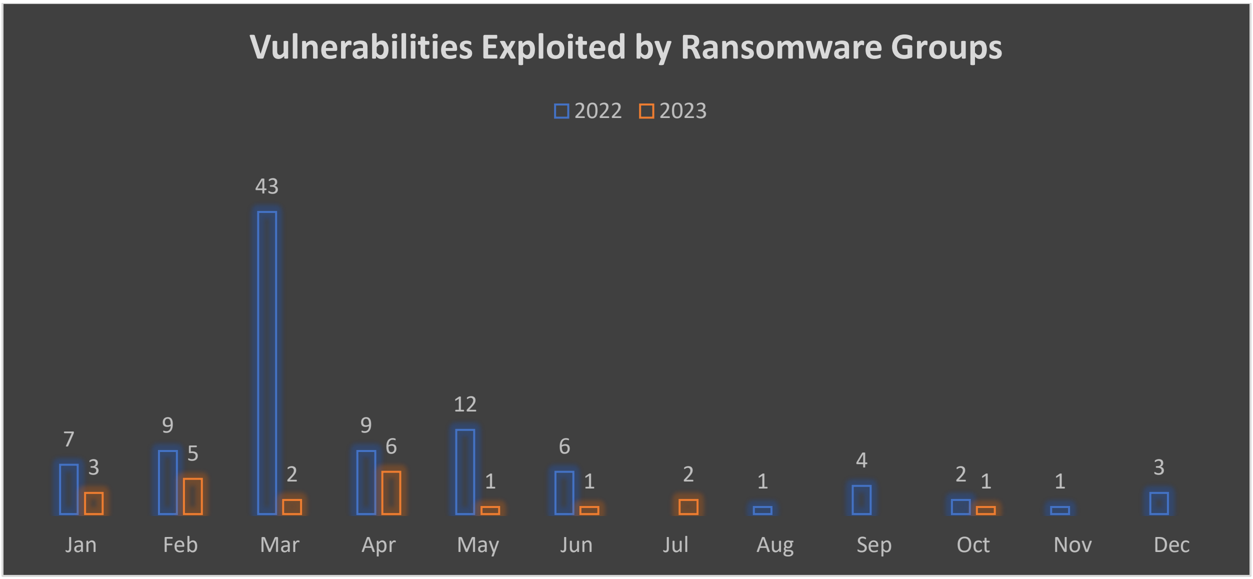
EXECUTIVE SUMMARY

Our investigation has unveiled the presence of critical vulnerabilities and exploits for sale on various dark forums and Telegram channels. These vulnerabilities encompass Elevation of Privilege, Authentication Bypass, SQL Injection, and Remote Code Execution, posing significant security risks. The affected platforms include Windows, JetBrains software, Microsoft Streaming Service Proxy, and Ubuntu kernels. One interesting finding is that Ransomware groups are actively searching for zero-day vulnerabilities in underground forums to compromise a large number of victims. To protect themselves, organizations must remain vigilant and prioritize security measures - including patch management and proactive threat monitoring - to safeguard against potential attacks.

INTRODUCTION

Our analysis of various deep web forums revealed a concerning abundance of discussions and transactions related to a wide range of vulnerabilities and exploits. These forums have become breeding grounds for threat actors seeking to buy, sell, or exchange knowledge and tools that could compromise digital security. Our findings underscore the pressing need for robust cybersecurity measures, intelligence sharing, and law enforcement efforts to counter the proliferation of these underground markets and protect organizations and individuals from emerging threats.

In 2023, CISA added approximately 159 vulnerabilities to the Known Exploited Vulnerabilities list. Of that number, 21 are exploited by ransomware groups, highlighting the exploitation to gain initial access, as well as lateral movement.



Even though the number of vulnerabilities exploited by ransomware groups in 2022 is less than 2023, they target vulnerabilities that can help them to exploit larger attack surfaces like MOVEit (CVE-2023-34362), PaperCut (CVE-2023-27350), and others.

KEY FINDINGS

- During our analysis, we discovered that many zero-day exploits were being sold on dark web forums. For instance, the Microsoft Streaming Server vulnerability (CVE-2023-36802) was available for purchase in February 2023, even though its CVE was officially assigned in September 2023.
- The MOVEit vulnerability led to the exposure of 62 million people to the attacks, resulting in approximately USD 950,000 in expenses related to cyber incidents and vulnerability response. Geographically, the impact of the MOVEit exploit extended to several countries, including the United States, Germany, France, the United Kingdom, Canada, and more.
- Similarly, the PaperCut vulnerability had a global impact, affecting more than 100 million users worldwide. Threat actors such as Lockit and Cl0p leveraged these exploits for their ransomware-as-a-service operations.

KEY VULNERABILITIES DISCUSSED

Our investigation in this report will cover the following critical vulnerabilities and their correlated external threat landscape so that cyber defenders are better prepared to address any possible external threats and risks posed by these vulnerabilities.

CVE-ID	CVE-Score	Product	NVD Published Date	Threat actor /Campaign
CVE-2023-28252	7.8	Microsoft	04/11/2023	Nokoyawa Ransomware
CVE-2023-27350	9.8	PaperCut	04/20/2023	Bl00dy Ransomware Gang/Cl0p ransomware
CVE-2023-34362	9.8	MOVEit	06/02/2023	Cl0p ransomware group
CVE-2023-3519	9.8	Citrix Systems	07/19/2023	Unknown
CVE-2023-2640	7.8	Ubuntu	07/25/2023	Unknown
CVE-2023-38831	7.8	WinRAR	08/23/2023	Konni APT
CVE-2023-36802	7.8	Microsoft	09/12/2023	Unknown
CVE-2023-42793	9.8	JetBrains	09/19/2023	North Korean threat actors
CVE-2023-40044	8.8	WS_FTP Server	09/27/2023	Cl0p threat actors

CVE-2023-28252 (WINDOWS CLFS ELEVATION OF PRIVILEGE) VULNERABILITY

- **Type:** Elevation of Privilege
- **CVSS Severity Score:** 7.8
- **Application:** Microsoft Windows Common Log File System
- **Impact:** Privilege Escalation, unauthorized access
- **Severity:** High
- **Patch Available:** Yes, April 11, 2023
- **Observed Exploitation by TA:** June 2022
- **Published in NVD:** April 11, 2023

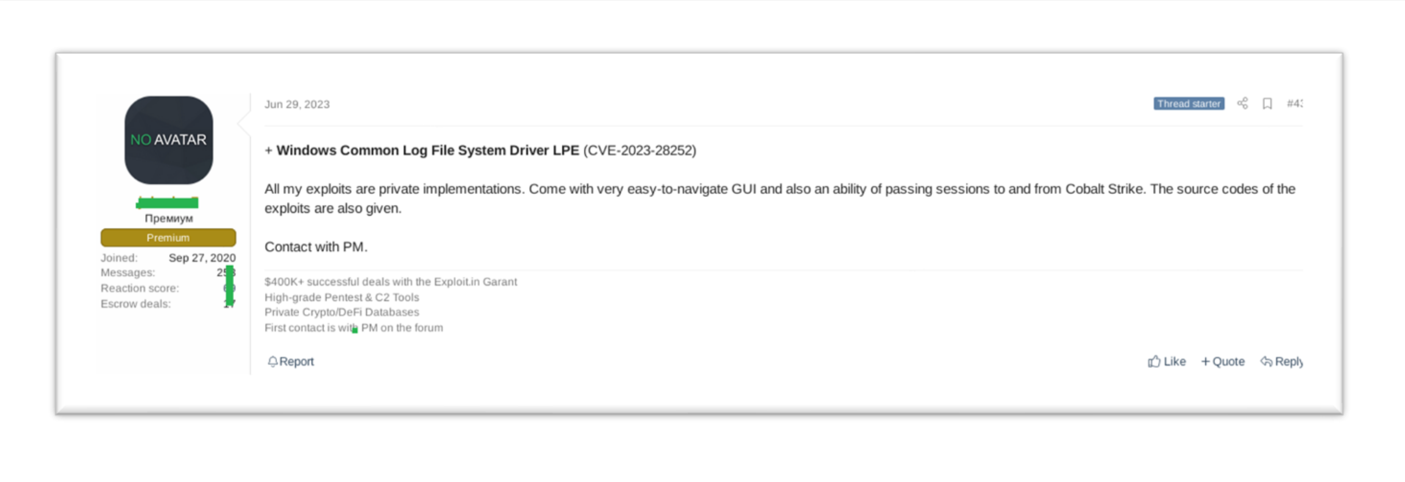
Affected Versions:

1. Windows Server 2008 R2 Build Number:- 6.1.7601.26466
2. Windows Server 2012 R2 Build Number:- 6.3.9600.20919
3. Windows Server 2016 Build Number:- 10.0.14393.5850
4. Windows Server 2019 Build Number:- 10.0.17763.4252
5. Windows Server 2022 Build Number:-10.0.20348.1668 and etc.

CVE-2023-28252 is a vulnerability found in the Windows Common Log File System (CLFS) that enables attackers to attain SYSTEM privileges on the target machines. This is a critical security issue as SYSTEM privileges provide the highest level of access and control on Windows systems.

Underground and Dark Web Forums

We observed a threat actor selling an exploit for a Microsoft Windows vulnerability (CVE-2023-2852) in an underground forum despite the patch being made available by Microsoft.



NO AVATAR

[redacted]

Премиум

Premium

Joined: Sep 27, 2020

Messages: [redacted]

Reaction score: [redacted]

Escrow deals: [redacted]

Jun 29, 2023

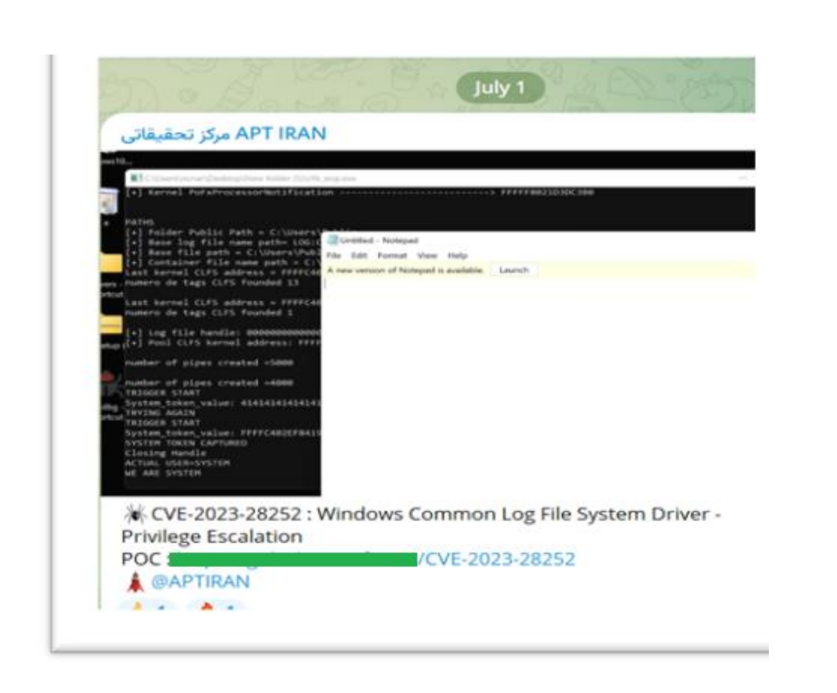
+ **Windows Common Log File System Driver LPE** (CVE-2023-28252)

All my exploits are private implementations. Come with very easy-to-navigate GUI and also an ability of passing sessions to and from Cobalt Strike. The source codes of the exploits are also given.

Contact with PM.

$400K+ successful deals with the Exploit.in Garant
High-grade Pentest & C2 Tools
Private Crypto/DeFi Databases
First contact is wit[redacted] PM on the forum

We observed Iranian threat actors discussing CVE-2023-2852 in a Telegram channel, highlighting their interest in active exploitation of the vulnerability.



July 1
Untitled - Notepad
File Edit Format View Help
A new version of Notepad is available. Launch

APT IRAN مرکز تحقیقاتی

```
[+] Kernel PofxProcessorNotification ---------------------------> FFFFF8021D3DC380


PATHS
[+] Folder Public Path = C:\Users\P
[+] Base log file name path= LOG:C
[+] Base file path = C:\Users\Publ
[+] Container file name path = C:\
Last kernel CLFS address = FFFFC40
numero de tags CLFS founded 13

Last kernel CLFS address = FFFFC40
numero de tags CLFS founded 1

[+] Log file handle: 00000000000000
[+] Pool CLFS kernel address: FFFF

number of pipes created =5000

number of pipes created =4000
TRIGGER START
System_token_value: 4141414141414141
TRYING AGAIN
TRIGGER START
System_token_value: FFFFC482EF841
SYSTEM TOKEN CAPTURED
Closing Handle
ACTUAL USER=SYSTEM
WE ARE SYSTEM
```

CVE-2023-28252 : Windows Common Log File System Driver - Privilege Escalation
POC [redacted]/CVE-2023-28252
@APTIRAN

Threat Actor

It was observed that the Nokoyawa ransomware group has been exploiting vulnerabilities in the CLFS driver since June 2022 (ahead of public availability in April 2023), using it to exploit retail, wholesale, energy, manufacturing, healthcare, software development and other sectors. Furthermore, exploit discussion in the underground forum and telegram channel highlights possible ongoing exploitation of unpatched servers.

CVE-2023-34362 (MOVEIT REMOTE CODE EXECUTION)

- **Vulnerability Type:** Remote code execution
- **CVSS Severity Score:** 9.8
- **Application:** MOVEit
- **Impact:** Unauthorized access, deserialization, remote code execution
- **Severity:** CRITICAL
- **Patched Available:** Yes, June 2023
- **Observed Exploitation by TA:** May 2023
- **Published in NVD:** June 02, 2023

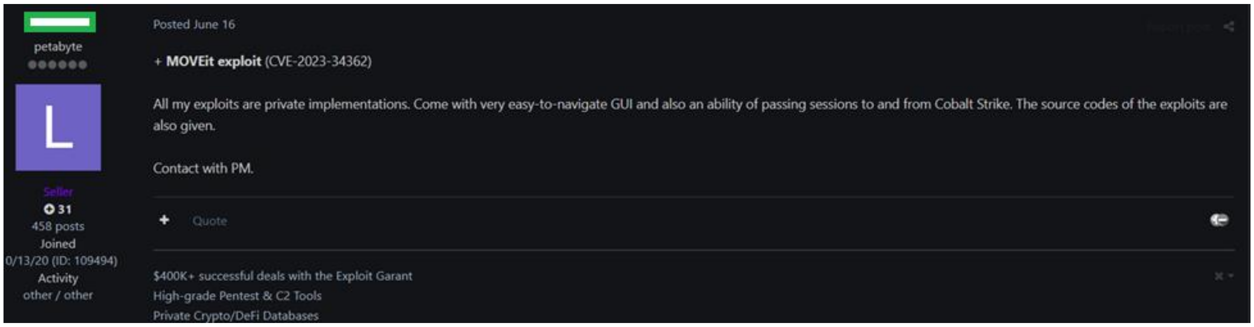
Affected Versions:

1. MOVEit Transfer 2023.0.0 (15.0)
2. MOVEit Transfer 2022.1.x (14.1)
3. MOVEit Transfer 2021.1.x (14.1)
4. MOVEit Transfer 2020.1.x (12.1) and older.

This vulnerability arises from inadequate sanitization of user-provided data, enabling unauthenticated remote attackers to illicitly access the MOVEit application. If successfully exploited, this vulnerability could empower remote attackers to read, delete, or alter database information and assume full control over the affected application. The exploitation can take place through either HTTP or HTTPS, presenting a substantial security risk. Notably, threat actors including Cl0p and LockBit, have utilized this as a zero-day exploit to compromise numerous victims globally.

Underground and Dark Web Forums

Recently, vulnerability in the MOVEit application created chaos worldwide. At the same time, we have observed a threat actor actively selling MOVEit exploit even after its patch had been released by Progress Software.



petabyte

Seller

31

458 posts

Joined

0/13/20 (ID: 109494)

Activity

other / other

Posted June 16

+ **MOVEit exploit** (CVE-2023-34362)

All my exploits are private implementations. Come with very easy-to-navigate GUI and also an ability of passing sessions to and from Cobalt Strike. The source codes of the exploits are also given.

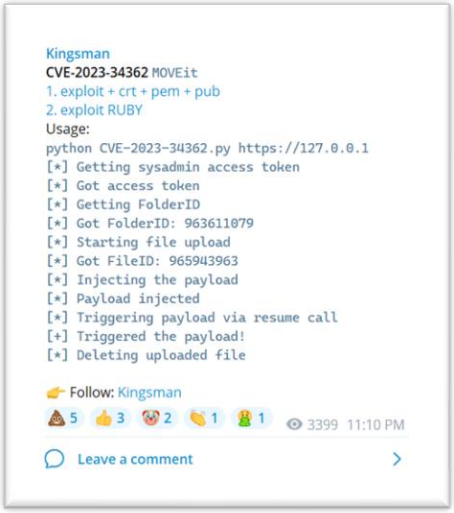
Contact with PM.

$400K+ successful deals with the Exploit Garant

High-grade Pentest & C2 Tools

Private Crypto/DeFi Databases

In Telegram channels, we found threads by threat actors discussing how to execute and compromise the victims' systems.



Kingsman

CVE-2023-34362 `MOVEit`

1. exploit + crt + pem + pub
2. exploit RUBY

Usage:

```
python CVE-2023-34362.py https://127.0.0.1
[*] Getting sysadmin access token
[*] Got access token
[*] Getting FolderID
[*] Got FolderID: 963611079
[*] Starting file upload
[*] Got FileID: 965943963
[*] Injecting the payload
[*] Payload injected
[*] Triggering payload via resume call
[+] Triggered the payload!
[*] Deleting uploaded file
```

👉 Follow: Kingsman

Threat Actor

The Cl0p ransomware group has used a zero-day vulnerability in the MOVEit application (CVE-2023-34362) to compromise numerous organizations around the world. Their ransom notes first appeared in May 2023, before Progress Software released a security advisory in June 2023. So far, Cl0p has targeted over 3,000 organizations in the US and 8,000 worldwide. Cl0p is a well-known RaaS (Ransomware-as-a-Service) operation with ties to Russia. Cl0p has a history of exploiting zero-day vulnerabilities, causing widespread damage in the ransomware landscape.

CITRIX ADC AND GATEWAY VULNERABILITIES

- **Vulnerability Type:** Remote code execution
- **CVSS Severity Score:** 9.8
- **Application:** Citrix ADC and Citrix Gateway
- **Impact:** Remote code execution, unauthorized access
- **Severity:** CRITICAL
- **Patched Available:** Yes, July 2023
- **Observed Exploitation by TA:** June 2023
- **Published in NVD:** June 19, 2023

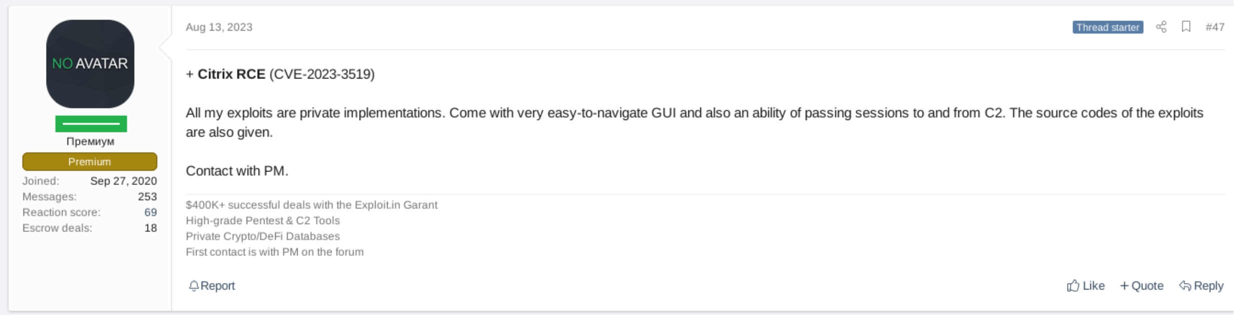
Affected Versions:

1. NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13
2. NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13
3. NetScaler ADC 13.1-FIPS before 13.1-37.159
4. NetScaler ADC 12.1-FIPS before 12.1-55.297
5. NetScaler ADC 12.1-NDcPP before 12.1-55.297

CVE-2023-3519 is a critical security vulnerability that affects Citrix ADC and Gateway products. This vulnerability permits attackers to execute malicious code remotely without requiring any form of authentication. In other words, attackers can compromise the targeted system, gain unauthorized access, and potentially steal sensitive information by exploiting this vulnerability.

Underground and Dark Web Forums

In our research on Citrix ADC and Gateway vulnerability, we observed that threat actors are not only marketing Citrix exploits but are also openly disseminating information on forums on identifying susceptible Citrix ADC systems by offering search engine filters.



Joined: Sep 27, 2020
Messages: 253
Reaction score: 69
Escrow deals: 18

Aug 13, 2023

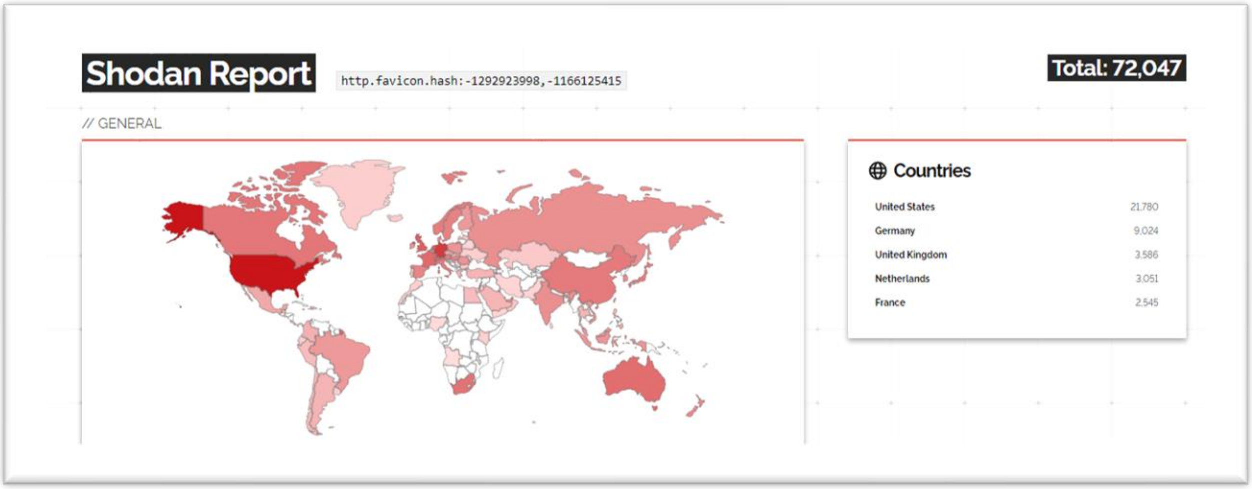
+ **Citrix RCE** (CVE-2023-3519)

All my exploits are private implementations. Come with very easy-to-navigate GUI and also an ability of passing sessions to and from C2. The source codes of the exploits are also given.

Contact with PM.

$400K+ successful deals with the Exploit.in Garant
High-grade Pentest & C2 Tools
Private Crypto/DeFi Databases
First contact is with PM on the forum

In our OSINT search, we found around, 72,000 devices Citrix systems publicly facing the internet, and this is a significant security concern, despite the patch being made available.



Shodan Report `http.favicon.hash:-1292923998,-1166125415` Total: 72,047

// GENERAL

Countries

United States	21,780
Germany	9,024
United Kingdom	3,586
Netherlands	3,051
France	2,545

Threat Actors

It was observed that threat actors used this as a zero-day vulnerability for exploitation. The attack was first identified in June 2023, after which Citrix released a security advisory and the patch in July 2023. The largest number of impacted IP addresses associated with Citrix ADC and Gateway vulnerability (CVE-2023-3519) are based in Germany, followed by France, Switzerland, Italy, Sweden, Spain, Japan, China, Austria, and Brazil.

CVE-2023-36802 (MICROSOFT STREAMING SERVICE PROXY ELEVATION OF PRIVILEGE)

- **Vulnerability Type:** Elevation of Privilege
- **CVSS Severity Score:** 7.8
- **Application:** Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability
- **Impact:** Privilege Escalation, Unauthorized Access
- **Severity:** HIGH
- **Patched Available:** Yes, September 2023
- **Observed Exploitation by TA:** Feb 2023
- **Published in NVD:** September 12, 2023

Affected Versions:

1. Windows Server 2019 Build Number:- 10.0.17763.4851
2. Windows Server 2022 Build Number:- 10.0.20348.1970
3. Windows 10 Build Number:-10.0.19044.3448
4. Windows 11 Build Number:-10.0.22000.2416

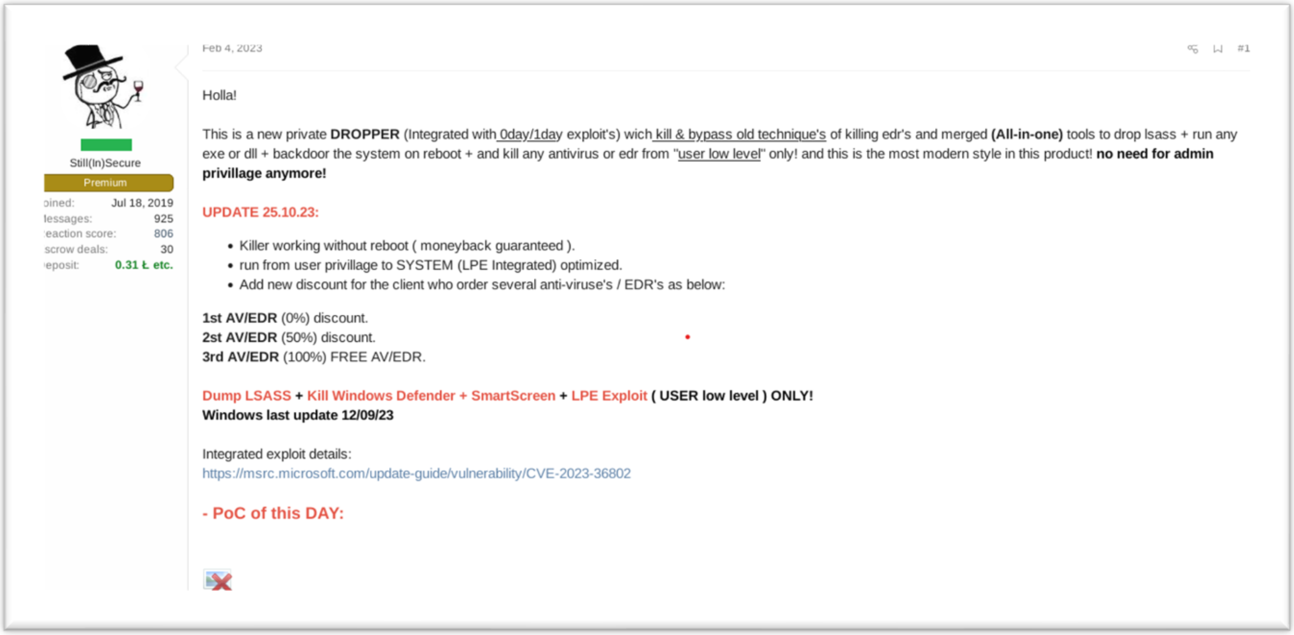
Microsoft Streaming Service Proxy vulnerability (CVE-2023-36802) allows attackers to gain SYSTEM privileges – once attackers have gained SYSTEM privileges, they can install, modify, or delete software and files without restrictions, as well as access sensitive system data.

Threat Actor

A well-known initial access broker "r1z" was engaged in the sale of an exploit for Microsoft Streaming Service Proxy (CVE-2023-36802) for a price ranging from USD 10,000 to USD 20,000. Previously threat actor was involved in selling exploits for various other vulnerabilities, such as those related to Atlassian Confluence Data Center, Microsoft SharePoint RCE Exploit CVE-2023-29357, and CVE-2023-40477 Winrar.

Underground and Dark Web Forums

CISA added a Microsoft Streaming Service Proxy vulnerability (CVE-2023-36802) in September 2023. On a dark forum, a well-known initial access broker was observed selling an exploit for the Microsoft Streaming Service Proxy vulnerability from February 2023. It had been actively sold on dark forums for seven months before Microsoft and CISA released an advisory on active exploitation.



Still(In)Secure

Premium

oined:	Jul 18, 2019
lessages:	925
eaction score:	806
scrow deals:	30
eposit:	0.31 Ł etc.

Feb 4, 2023

#1

Holla!

This is a new private **DROPPER** (Integrated with 0day/1day exploit's) wich kill & bypass old technique's of killing edr's and merged **(All-in-one)** tools to drop lsass + run any exe or dll + backdoor the system on reboot + and kill any antivirus or edr from "user low level" only! and this is the most modern style in this product! **no need for admin privillage anymore!**

UPDATE 25.10.23:

- Killer working without reboot (moneyback guaranteed).
- run from user privillage to SYSTEM (LPE Integrated) optimized.
- Add new discount for the client who order several anti-viruse's / EDR's as below:

1st AV/EDR (0%) discount.
2st AV/EDR (50%) discount.
3rd AV/EDR (100%) FREE AV/EDR.

Dump LSASS + Kill Windows Defender + SmartScreen + LPE Exploit (USER low level) ONLY!
Windows last update 12/09/23

Integrated exploit details:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36802

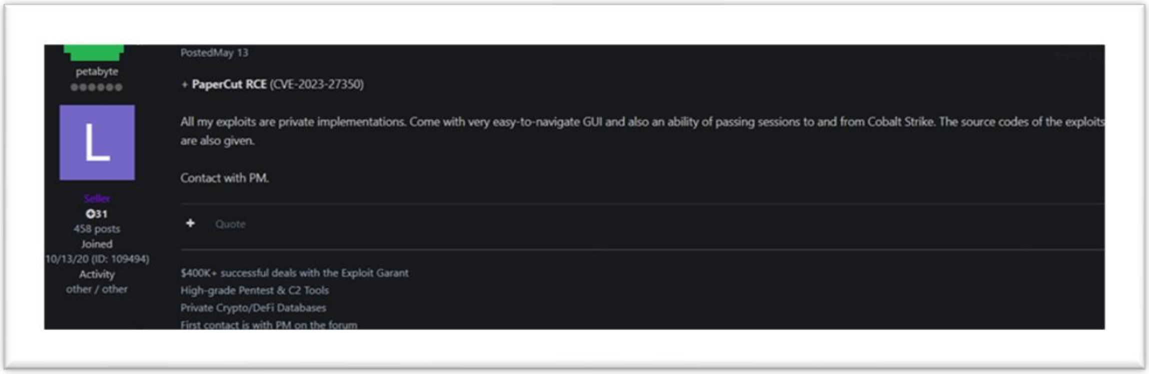
- PoC of this DAY:

PAPERCUT VULNERABILITIES

- **Vulnerability Type:** Remote code execution
- **CVSS Severity Score:** 9.8
- **Application:** PaperCut
- **Impact:** Remote code execution, unauthorized access
- **Severity:** CRITICAL
- **Patched Available:** Yes, April 2023
- **Observed Exploitation by TA**: May 2023
- **Published in NVD:** April 20, 2023

Underground and Dark Web Forums

On the underground forum, the exploit for the PaperCut vulnerability continues to be sold, one month after the patch release, and threat actors are still actively using this exploit.



petabyte
Seller
31
458 posts
Joined 10/13/20 (ID: 109494)
Activity
other / other

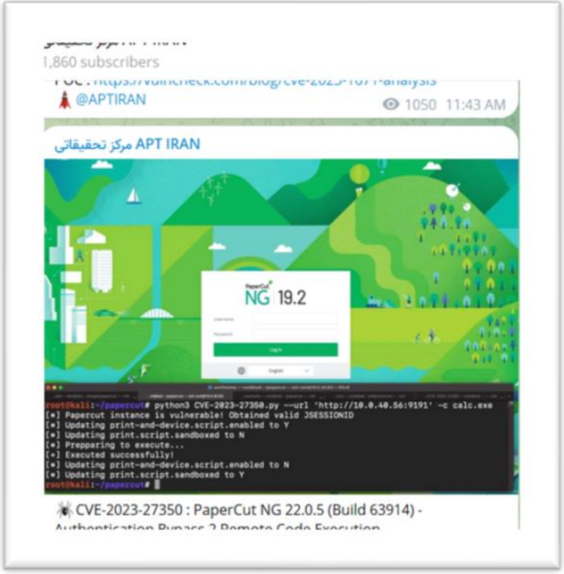
PostedMay 13

+ **PaperCut RCE** (CVE-2023-27350)

All my exploits are private implementations. Come with very easy-to-navigate GUI and also an ability of passing sessions to and from Cobalt Strike. The source codes of the exploits are also given.

Contact with PM.

$400K+ successful deals with the Exploit Garant
High-grade Pentest & C2 Tools
Private Crypto/DeFi Databases
First contact is with PM on the forum



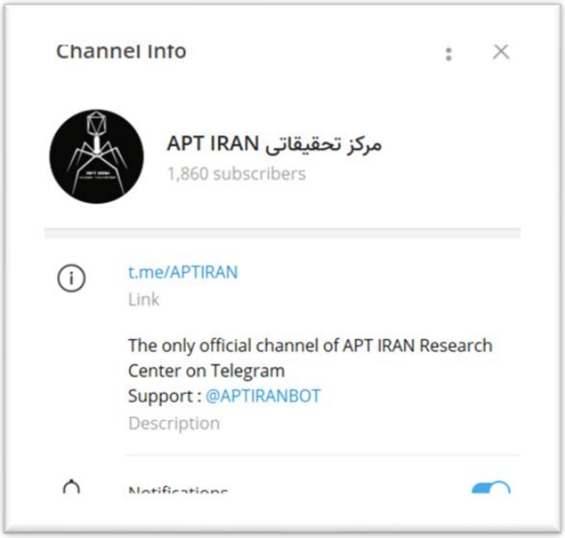
1,860 subscribers

PoC : https://vulncheck.com/blog/cve-2023-1071-analysis
@APTIRAN

APT IRAN مرکز تحقیقاتی

```
root@kali:~/papercut# python3 CVE-2023-27350.py --url 'http://10.0.40.56:9191' -c calc.exe
[*] Papercut instance is vulnerable! Obtained valid JSESSIONID
[*] Updating print-and-device.script.enabled to Y
[*] Updating print.script.sandboxed to N
[*] Prepparing to execute...
[*] Executed successfully!
[*] Updating print-and-device.script.enabled to N
[*] Updating print.script.sandboxed to Y
root@kali:~/papercut#
```

CVE-2023-27350 : PaperCut NG 22.0.5 (Build 63914) - Authentication Bypass ? Remote Code Execution



APT IRAN مرکز تحقیقاتی
1,860 subscribers

t.me/APTIRAN
Link

The only official channel of APT IRAN Research Center on Telegram
Support : @APTIRANBOT
Description

Affected Versions:

1. PaperCut MF or PaperCut NG version 8.0 or later, on all OS platforms
2. PaperCut MF or PaperCut NG Application Servers
3. PaperCut MF or PaperCut NG Site Servers

PaperCut is a print management software developed in Java, designed to support multi-server and multi-operating system environments. In a typical deployment, there is a primary server that acts as the main application server, and secondary servers that runs as a lightweight monitoring component.

Threat Actors

Multiple ransomware groups, including Cl0p, have been identified using this exploit. In May 2023, the Bl00dy ransomware gang specifically targeted vulnerable PaperCut servers in various sectors, including education, IT, and a range of small and large-scale industries. The company claims to have affected over 100 million users. Notably, we've observed that since the patch was released, the vulnerability has not been exploited.

CVE-2023-38831 (WINRAR REMOTE CODE EXECUTION)

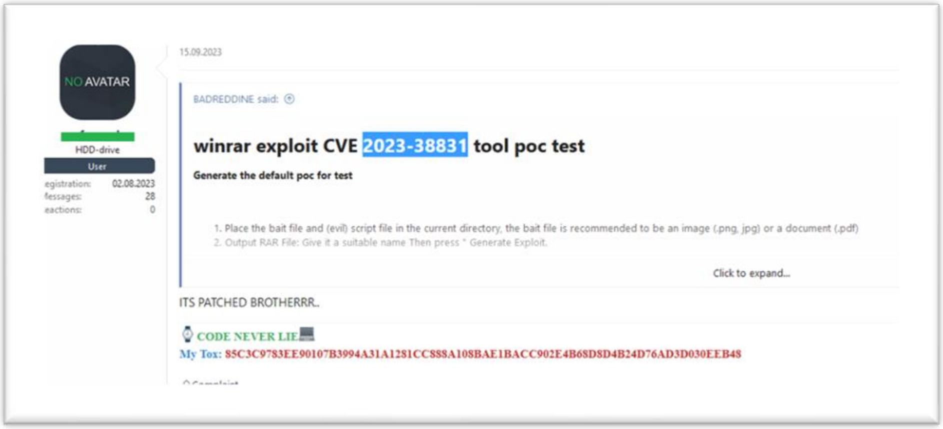
- **Vulnerability Type:** Remote code execution
- **CVSS Severity Score:** 7.8
- **Application:** WinRAR
- **Impact:** Remote code execution, unauthorized access
- **Severity:** HIGH
- **Patched Available:** Yes, August 2023
- **Observed Exploitation by TA:** April 2023
- **Published in NVD:** August 23, 2023

Affected Versions: WinRAR before 6.23

This zero-day vulnerability (CVE-2023-38831) in WinRAR, allows hackers to install malware through manipulated archives, exposing users to hidden malicious scripts. The vulnerability enables attackers to execute arbitrary code when a user attempts to view what appears to be a harmless file, such as an ordinary PNG image file, within a ZIP archive.

Underground and Dark Web Forums

In an underground forum, we discovered that the WinRAR (CVE-2023-38831) vulnerability is actively being sold, even though a patch is available for it.



egistration:	02.08.2023
fessages:	28
eactions:	0

15.09.2023

BADREDDINE said:

winrar exploit CVE 2023-38831 tool poc test

Generate the default poc for test

1. Place the bait file and (evil) script file in the current directory, the bait file is recommended to be an image (.png, jpg) or a document (.pdf)
2. Output RAR File: Give it a suitable name Then press " Generate Exploit.

Click to expand...

ITS PATCHED BROTHERRR..

CODE NEVER LIE
My Tox: 85C3C9783EE90107B3994A31A1281CC888A108BAE1BACC902E4B68D8D4B24D76AD3D030EEB48

Threat Actors

The Konni APT; a North Korean state-sponsored cyber espionage group, as well as state-backed threat actors from Russia and China, have been exploiting a WinRAR vulnerability. Since April, threat actors have been using this vulnerability, potentially impacting over 500 million users worldwide. This exploitation has enabled the distribution of various malware families, including DarkMe, GuLoader, and Remcos RAT.

CVE-2023-2640 (UBUNTU ELEVATION OF PRIVILEGE)

- **Vulnerability Type:** Elevation of Privilege
- **CVSS Severity Score:** 7.8 HIGH
- **Application:** Ubuntu
- **Impact:** Elevation of privilege
- **Severity:** HIGH
- **Patched Available:** Yes, July 2023
- **Observed Exploitation by TA:** September 2023
- **Published in NVD:** August 03, 2023

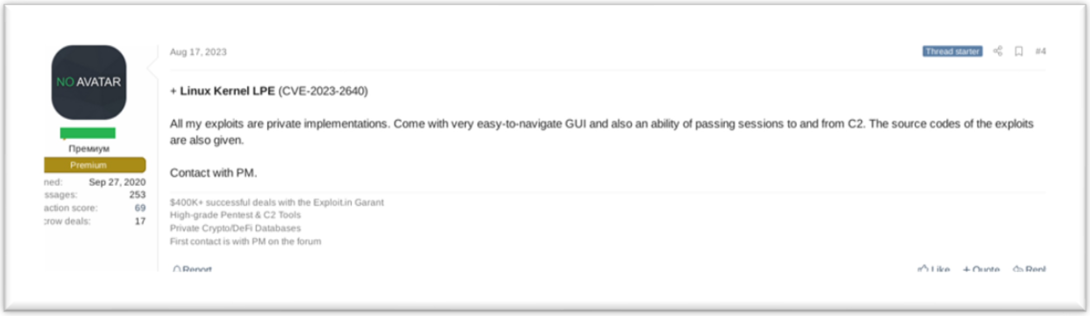
Affected Versions:

1) 6.2. Ubuntu 23.04 (Lunar Lobster) / Ubuntu 22.04 LTS (Jammy Jellyfish)
2) 5.19.0 Ubuntu 22.10 (Kinetic Kudu) / Ubuntu 22.04 LTS (Jammy Jellyfish)
3) 5.4.0 Ubuntu 22.04 LTS (Local Fossa) / Ubuntu 18.04 LTS (Bionic Beaver)

The vulnerability CVE-2023-2640 in certain Ubuntu kernels enables unprivileged users to set privileged extended attributes on mounted files without undergoing the necessary security checks. The GameOver(lay) vulnerabilities enable the crafting of an executable file with scoped file capabilities, tricking the Ubuntu Kernel into copying it to a different location with un-scoped capabilities. This grants anyone executing it root privileges.

Underground and Dark Web Forums

CVE-2023-2640; a vulnerability in the Ubuntu Kernel, has been observed for sale on the Dark forum. Threat actors continue to exploit this vulnerability even after a patch has become available.



Aug 17, 2023

+ **Linux Kernel LPE** (CVE-2023-2640)

All my exploits are private implementations. Come with very easy-to-navigate GUI and also an ability of passing sessions to and from C2. The source codes of the exploits are also given.

Contact with PM.

$400K+ successful deals with the Exploit.in Garant
High-grade Pentest & C2 Tools
Private Crypto/DeFi Databases
First contact is with PM on the forum

ned:	Sep 27, 2020
ssages:	253
action score:	69
:row deals:	17

Threat Actors

Threat actors continue to sell the exploits even after its patch was available. The Ubuntu Kernel vulnerability affects 40% of Ubuntu cloud workloads.

CVE-2023-42793 (JETBRAINS UNAUTHENTICATED RCE)

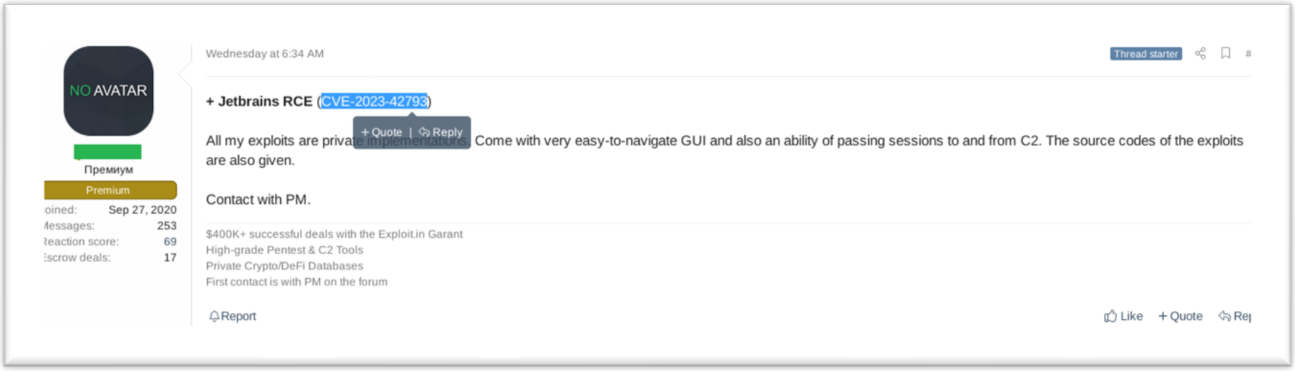
- **Vulnerability Type:** Unauthenticated RCE Vulnerabilities
- **CVSS Severity Score:** 9.8 CRITICAL
- **Application:** JetBrains
- **Impact:** Authentication bypass
- **Severity:** HIGH
- **Patched Available:** Yes, September 2023
- **Observed Exploitation by TA:** October 2023
- **Published in NVD:** September 19, 2023

Affected Versions: JetBrains TeamCity Prior to 2023.05.4

The Jet Brains vulnerability (CVE-2023-42793) enables an unauthenticated attacker to gain access to a TeamCity server, allowing them to execute remote code and potentially leading to the compromise of source code and the potential for further supply chain attacks.

Underground and Dark Web Forums

While exploring various dark forums, we observed a trade involving an exploit for JetBrains software (CVE-2023-42793).



oined: Sep 27, 2020
lessages: 253
leaction score: 69
Escrow deals: 17

Wednesday at 6:34 AM

+ Jetbrains RCE (CVE-2023-42793)

All my exploits are private implementations. Come with very easy-to-navigate GUI and also an ability of passing sessions to and from C2. The source codes of the exploits are also given.

Contact with PM.

$400K+ successful deals with the Exploit.in Garant
High-grade Pentest & C2 Tools
Private Crypto/DeFi Databases
First contact is with PM on the forum

Threat Actors

Since early October 2023, Microsoft has observed North Korean nation-state threat actors Diamond Sleet and Onyx Sleet exploiting the Jet Brains TeamCity CVE-2023-42793 remote-code execution vulnerability. These nation-state threat actors use this vulnerability to install malware and backdoors.

CVE-2023-40044 (WS_FTP SERVER .NET DESERIALIZATION)

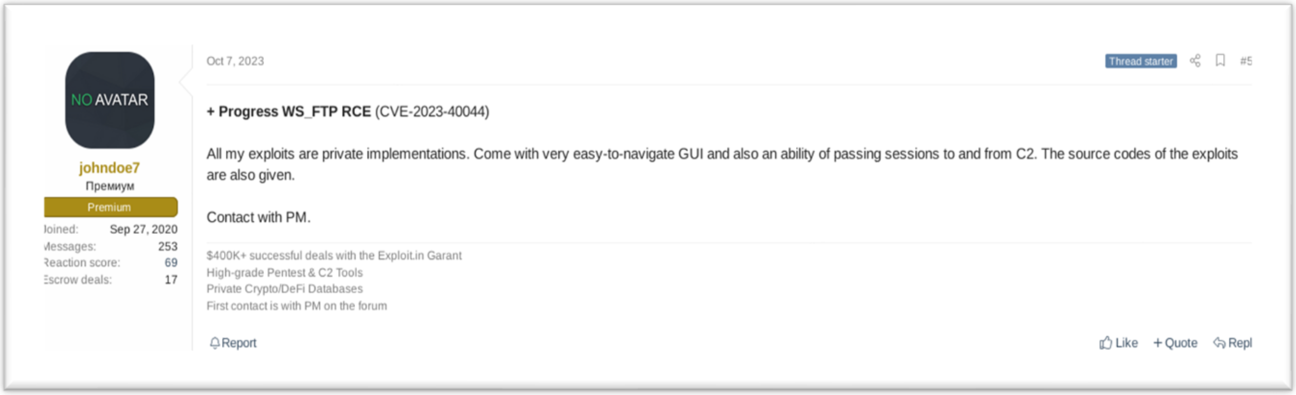
- **Vulnerability Type:** NET deserialization vulnerability
- **CVSS Severity Score:** 8.8 HIGH
- **Application:** Progress Software Corporation WS_FTP Server
- **Impact:** Authentication bypass
- **Severity:** HIGH
- **Patched Available:** Yes, September 2023
- **Observed Exploitation by TA:** October 2023
- **Published in NVD:** September 27, 2023

Affected Versions: WS_FTP Server Versions Prior to 8.7.4 and 8.8.2

CVE-2023-40044 of the Transfer module is vulnerable to a .NET deserialization vulnerability that allows an unauthenticated attacker to execute remote commands on the WS_FTP Server operating system.

Underground and Dark Web Forums

CYFIRMA researchers discovered WS_FTP Server (CVE-2023-40044) for sale, after the patch was released.



+ Progress WS_FTP RCE (CVE-2023-40044)

All my exploits are private implementations. Come with very easy-to-navigate GUI and also an ability of passing sessions to and from C2. The source codes of the exploits are also given.

Contact with PM.

$400K+ successful deals with the Exploit.in Garant
High-grade Pentest & C2 Tools
Private Crypto/DeFi Databases
First contact is with PM on the forum

Threat Actor

The Cl0p threat actor uses the WS_FTP Server (CVE-2023-40044) vulnerability to target organizations across various sectors, from IT, to legal, oil and gas, and healthcare.

EXTERNAL THREAT LANDSCAPE MANAGEMENT

These vulnerabilities can affect organizations across all aspects of society. Threat actors with knowledge of these vulnerabilities may selectively target industries based on the perceived value of the data, or services handled by these software instances. Organizations dealing with sensitive data or those heavily dependent on these tools may particularly be attractive targets.

To effectively manage the external threat landscape, organizations can benefit from cyber threat intelligence services. These services provide real-time information on emerging threats, vulnerabilities, and attack trends, allowing organizations to stay one step ahead of potential attackers.

CONCLUSION

This report highlights several critical vulnerabilities (CVEs) and their potential implications, covering a wide range of software and systems. Their criticality underscores the importance of prompt action and mitigation, making timely patching, upgrading, and vigilant security practices essential to prevent exploitation and mitigate risks.

STRATEGIC RECOMMENDATIONS

Training and Awareness: regularly conduct cybersecurity training for employees to educate them about phishing, social engineering, and safe online practices.

Applying Security Patches and Updating Software: regularly applying security patches and updating software installations is the first line of defence against technical vulnerabilities, ensuring known vulnerabilities are promptly addressed.

Risk Recover Planning: Develop and consistently update a comprehensive incident response plan to ensure a swift and effective response in the event of a ransomware attack, with the goal of minimizing potential impact and downtime.

MANAGEMENT RECOMMENDATIONS

Security Audits: Periodically conduct security audits and assessments to identify and rectify potential weaknesses in the organization's infrastructure and processes.

Legal and Regulatory Compliance: Stay informed about evolving data protection laws and regulations and ensure compliance to mitigate potential legal repercussions, following a vulnerabilities Exploitation incident.

TACTICAL RECOMMENDATIONS

Phishing Mitigation: Employing anti-phishing solutions and email filtering to detect and block malicious phishing emails is essential. User education on how to recognize and report phishing attempts can also play a vital role in preventing successful attacks.

Asset Inventory and Vulnerability Scanning: Maintain an accurate and up-to-date inventory of all systems, software, and devices in your environment. Implement regular vulnerability scanning to identify and assess vulnerabilities on your network.

Data Backup: Ensure robust backup and disaster recovery solutions are in place to restore critical systems and data in case of a successful attack.