Mass Scanning For VMWare vCenter RCE

Weaponized exploits and mass scanning activity for two critical vCenter vulnerabilities

JUNE 7, 2021

Attackers are actively scanning for two critical remote command execution (RCE) vulnerabilities in VMWare vCenter servers. The first vulnerability, tracked as **CVE-2021-21972**, allows remote malicious actors unrestricted access to the host operating system. The vulnerability has a critical score of 9.8 and was disclosed in February of this year. Functioning proof of concepts and mass scanning activity followed within a few days after the disclosure. Recently, the vulnerability has been found weaponized by cryptomining Python botnet "Necro."

The second RCE vulnerability, tracked as **CVE-2021-21985**, also allows remote actors unrestricted access to the host operating system and also has a critical score of 9.8. The vulnerability was disclosed on May 25th, and by June 2nd, a blog post surfaced with technical details of the exploit. The details for weaponization of CVE-2021-21985 have only been available for three days at the time of writing and malicious activity is ramping up quickly.

vSphere servers are a hot commodity for malicious actors as they reside inside enterprise networks or virtual private clouds and provide reasonably large amounts of CPU and memory resources. From cryptojacking and ransomware to leveraging as malicious infrastructure or as a jump host for lateral movement and espionage/extortion, vulnerable and exposed servers are easily located and will be abused by malicious actors.

CVE-2021-21972

On February 23, 2021, VMWare **disclosed** a RCE vulnerability through the vSphere HTML5 client in a vCenter Server plugin. The severity of the issue was evaluated to be critical with a CVSSv3 score of 9.8. A malicious actor with network access to the server could exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts the vCenter Server. The privately reported vulnerability was disclosed simultaneously with a patch that fixed the issue in advisory **VMSA-2021-0002**.

On February 24, 2021, Mikhail Klyuchnikov of Positive Technologies **published** detailed results of his research from the autumn of 2020 that led to the discovery of the vulnerability. Positive Technologies originally planned to delay the release of the technical details to give organizations time to patch their vCenter servers, but after two functioning PoC exploits were already released and attackers started scanning for unpatched servers, they published earlier.

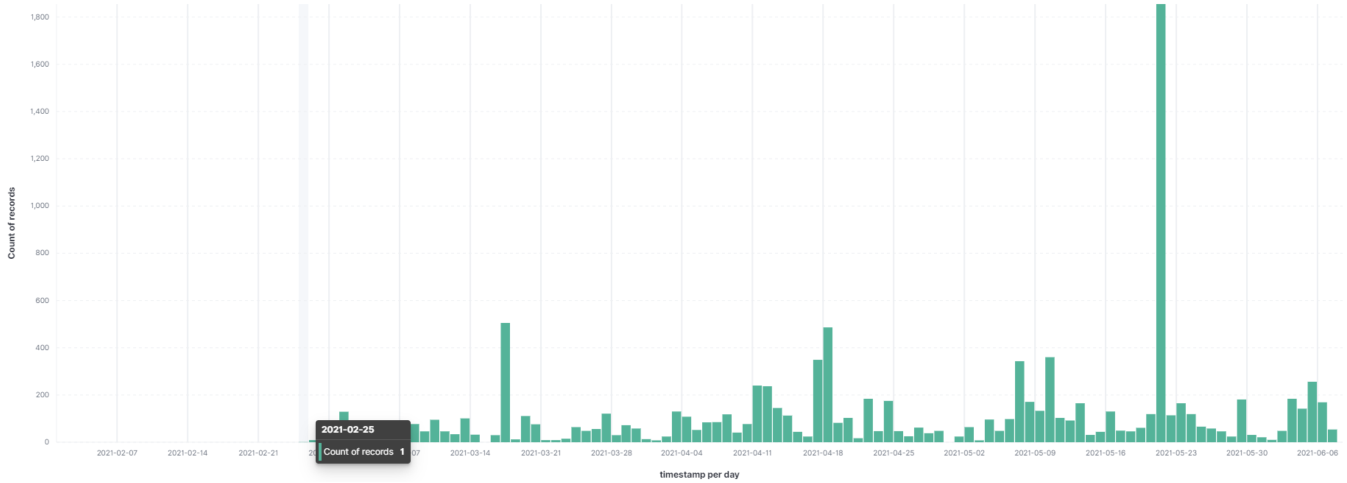


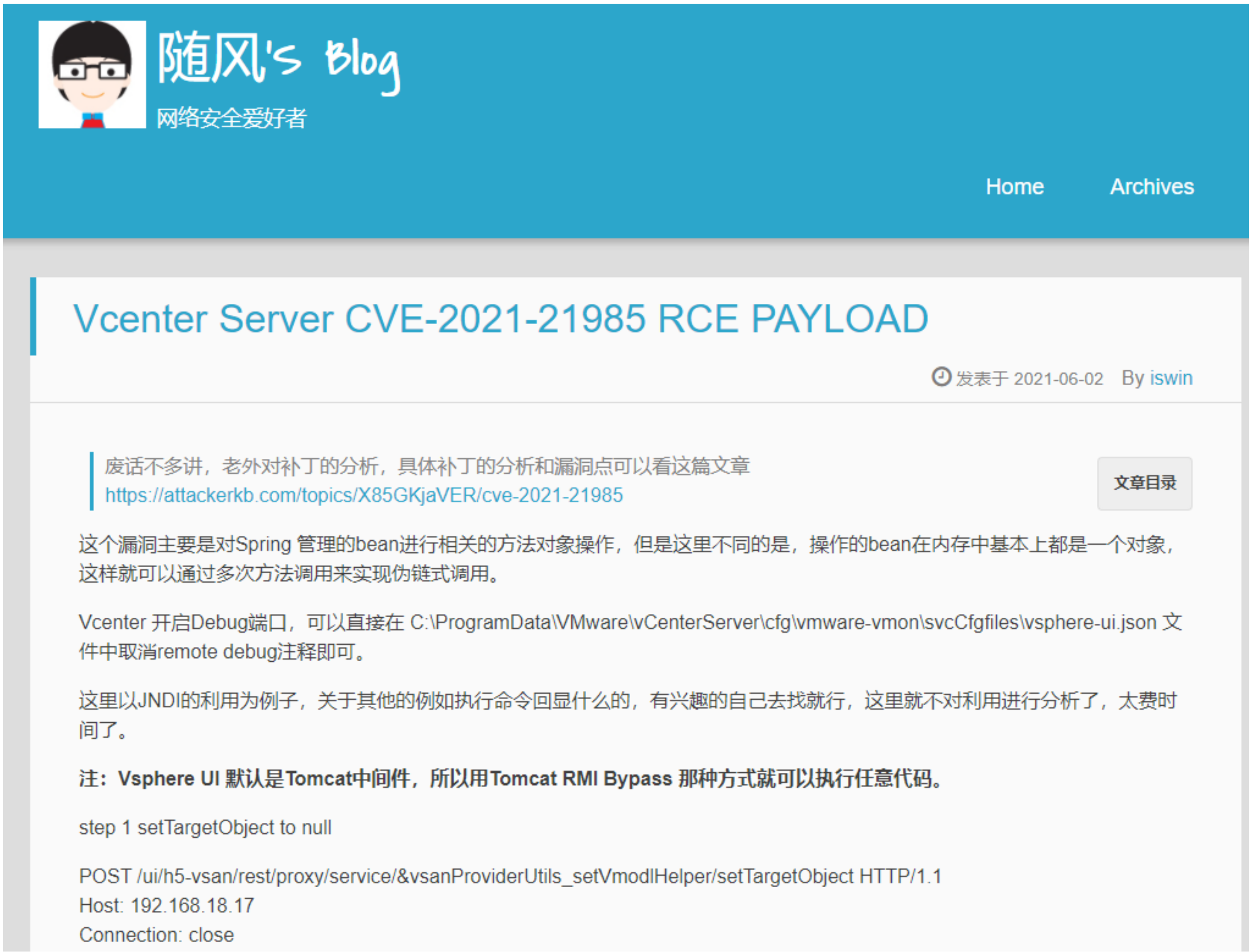
Figure 1: Scanning activity for CVE-2021-21972; first event detected on Feb 25, 2021

On June 3, 2021, Talos **reported** the addition of CVE-2021-21972 in the list of exploits leveraged by the Necro Python botnet since May 11th. Necro has been in development since 2015 and recently received significant updates as documented by **Check Point Research** and **Netlab360** in January of 2021. Necro is known to abuse systems to mine for Monero (XMR) and Tezos (XTZ) cryptocurrencies.

CVE-2021-21985

On May 25, 2021, VMWare **disclosed** a remote code execution vulnerability due to lack of input validation in the vSAN Health Check plugin. The affected Virtual SAN Health Check plugin is enabled in all vCenter server deployments, regardless of vSAN being used or not. The issue was evaluated as critical with a CVSSv3 score of 9.8. A malicious actor with network access to vCenter could exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts the vCenter Server. VMWare released patches to address the critical security issue through advisory **VMSA-2021-0010**.

On June 2, 2021, a post on **Windy's Blog** revealed enough details for any actor to weaponize the remote code execution in an exploit.



Vcenter Server CVE-2021-21985 RCE PAYLOAD

发表于 2021-06-02 By iswin

> 废话不多讲，老外对补丁的分析，具体补丁的分析和漏洞点可以看这篇文章
> https://attackerkb.com/topics/X85GKjaVER/cve-2021-21985

这个漏洞主要是对Spring 管理的bean进行相关的方法对象操作，但是这里不同的是，操作的bean在内存中基本上都是一个对象，这样就可以通过多次方法调用来实现伪链式调用。

Vcenter 开启Debug端口，可以直接在 C:\ProgramData\VMware\vCenterServer\cfg\vmware-vmon\svcCfgfiles\vsphere-ui.json 文件中取消remote debug注释即可。

这里以JNDI的利用为例子，关于其他的例如执行命令回显什么的，有兴趣的自己去找就行，这里就不对利用进行分析了，太费时间了。

注：Vsphere UI 默认是Tomcat中间件，所以用Tomcat RMI Bypass 那种方式就可以执行任意代码。

step 1 setTargetObject to null

```
POST /ui/h5-vsan/rest/proxy/service/&vsanProviderUtils_setVmodlHelper/setTargetObject HTTP/1.1
Host: 192.168.18.17
Connection: close
```

Figure 2: Windy's blog post on CVE-2021-21985 RCE payload

By June 1st, Radware's deception network recorded the first random scan events for CVE-2021-21985 and witnessed it escalate quickly over the next several days.

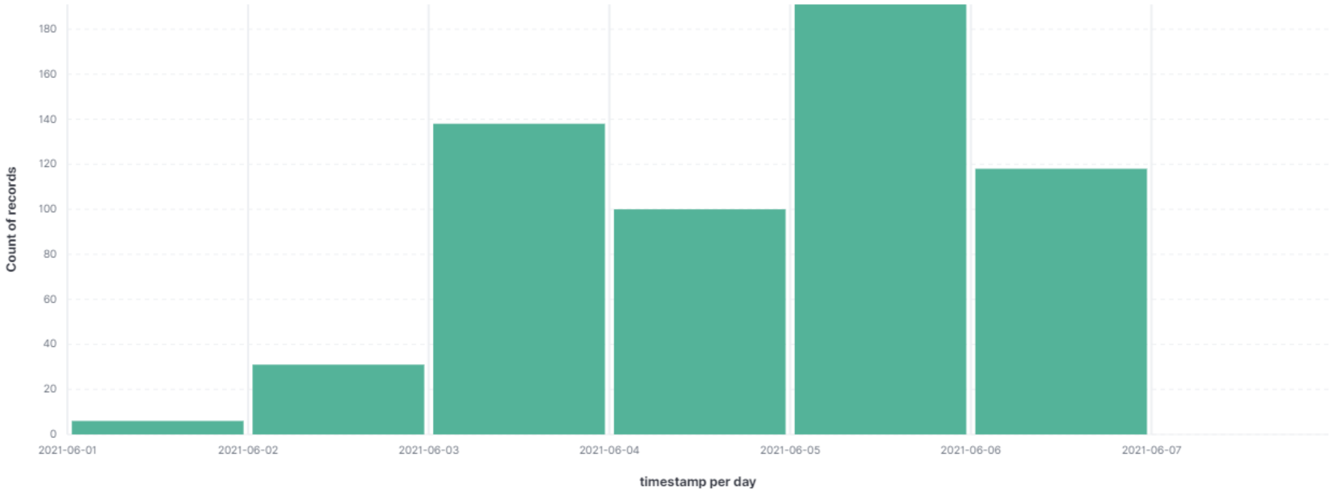
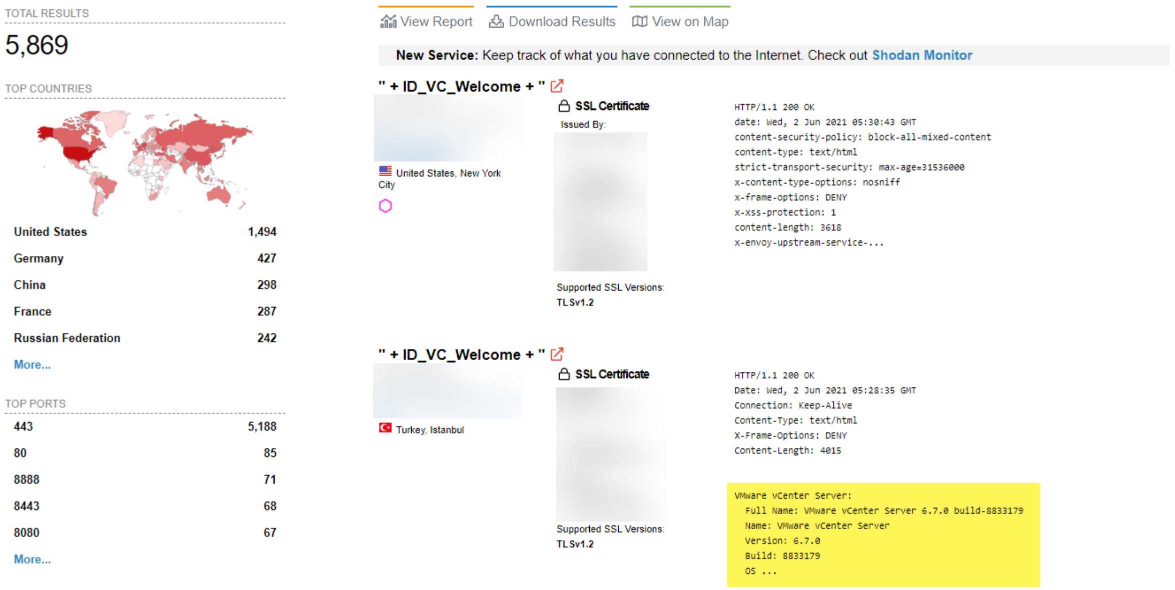


Figure 3: Scanning activity for CVE-2021-21985

Scanning For Vulnerabilities

While we detected scanning efforts by more sophisticated malicious actors seeking to exploit these vulnerabilities, less sophisticated actors can easily leverage a multitude of IoT search engines that provide this service to the masses. For a small fee, anyone can access and leverage the APIs offered by internet scanning engines, such as Shodan, ZoomEye and Censys, for automating vulnerability assessments of exposed VMWare vSphere servers.



TOTAL RESULTS

5,869

TOP COUNTRIES

United States	1,494
Germany	427
China	298
France	287
Russian Federation	242

More...

TOP PORTS

443	5,188
80	85
8888	71
8443	68
8080	67

More...

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

" + ID_VC_Welcome + "

United States, New York City

SSL Certificate

Issued By:

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
date: Wed, 2 Jun 2021 05:30:43 GMT
content-security-policy: block-all-mixed-content
content-type: text/html
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1
content-length: 3618
x-envoy-upstream-service-...
```

" + ID_VC_Welcome + "

Turkey, Istanbul

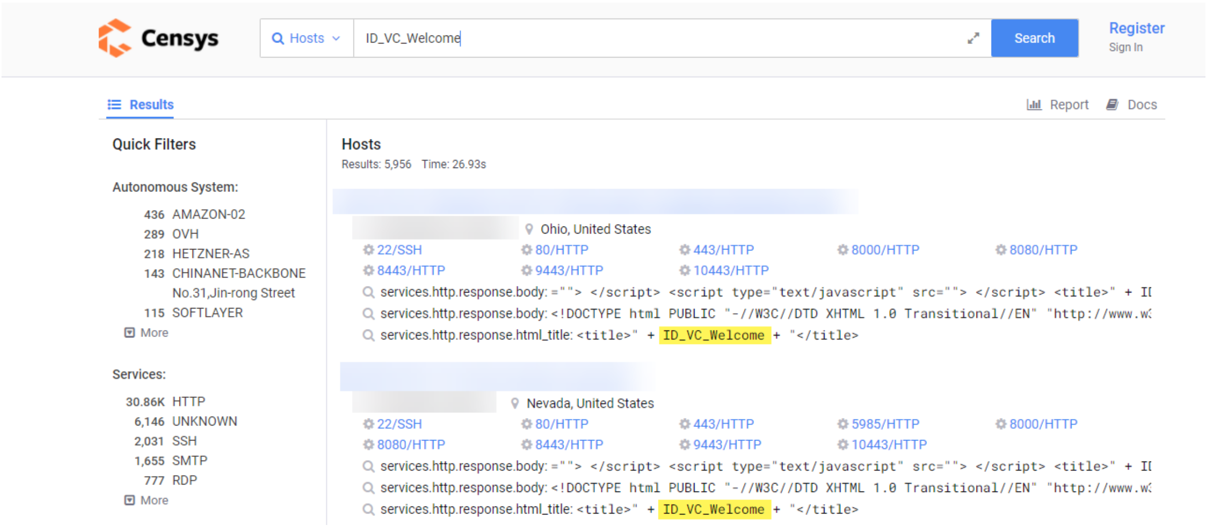
SSL Certificate

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
Date: Wed, 2 Jun 2021 05:28:35 GMT
Connection: Keep-Alive
Content-Type: text/html
X-Frame-Options: DENY
Content-Length: 4015

VMware vCenter Server:
  Full Name: VMware vCenter Server 6.7.0 build-8833179
  Name: VMware vCenter Server
  Version: 6.7.0
  Build: 8833179
  OS ...
```

Figure 4: Shodan vCenter Server search - free tier account (dd June 4, 2021)



Search: ID_VC_Welcome

Quick Filters

Autonomous System:

436	AMAZON-02
289	OVH
218	HETZNER-AS
143	CHINANET-BACKBONE No.31,Jin-rong Street
115	SOFTLAYER

More

Services:

30.86K	HTTP
6,146	UNKNOWN
2,031	SSH
1,655	SMTP
777	RDP

More

Hosts

Results: 5,956 Time: 26.93s

Ohio, United States

22/SSH 80/HTTP 443/HTTP 8000/HTTP 8080/HTTP
8443/HTTP 9443/HTTP 10443/HTTP

```
services.http.response.body: ="">  </script>  <script type="text/javascript" src=""> </script> <title>" + II
services.http.response.body: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3
services.http.response.html_title: <title>" + ID_VC_Welcome + "</title>
```

Nevada, United States

22/SSH 80/HTTP 443/HTTP 5985/HTTP 8000/HTTP
8080/HTTP 8443/HTTP 9443/HTTP 10443/HTTP

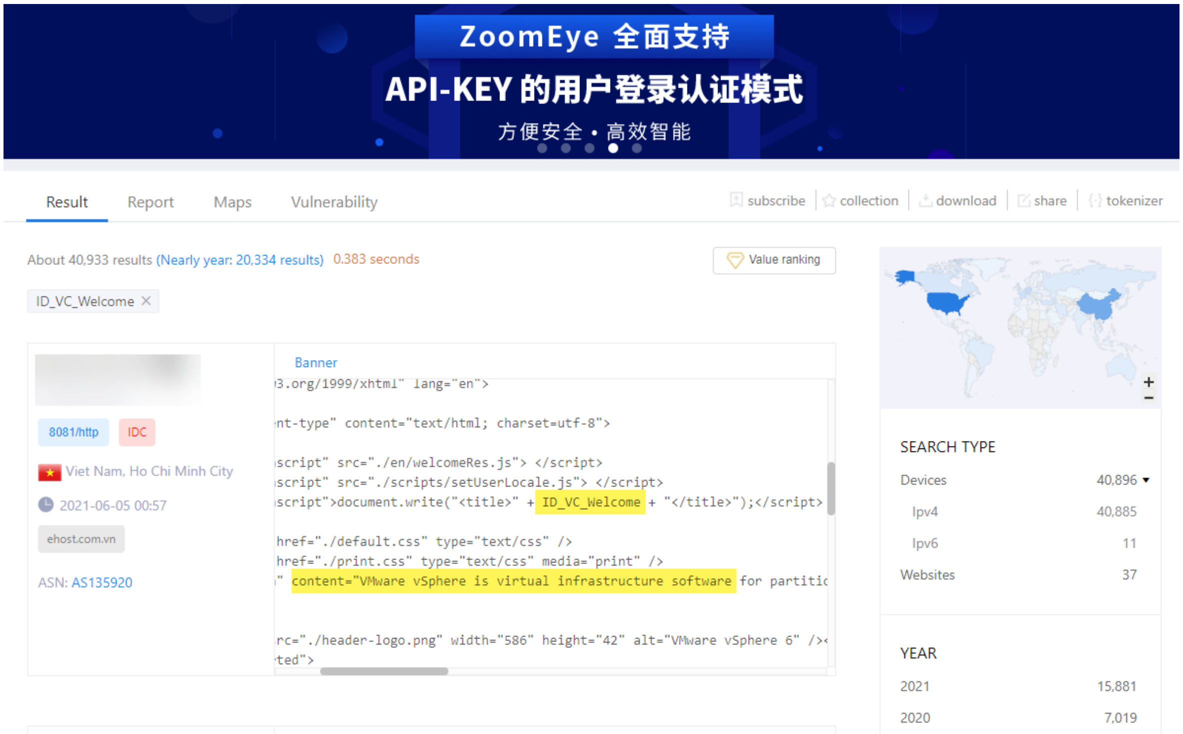
```
services.http.response.body: ="">  </script>  <script type="text/javascript" src=""> </script> <title>" + II
services.http.response.body: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3
services.http.response.html_title: <title>" + ID_VC_Welcome + "</title>
```

Figure 5: Censys vCenter server search - unregistered (dd June 4, 2021)

Mass Scanning For VMWare vCenter RCE

Weaponized exploits and mass scanning activity for two critical vCenter vulnerabilities

JUNE 7, 2021



ZoomEye 全面支持
API-KEY 的用户登录认证模式
方便安全 • 高效智能

About 40,933 results (Nearly year: 20,334 results) 0.383 seconds

ID_VC_Welcome ✕

8081/http IDC

Viet Nam, Ho Chi Minh City

2021-06-05 00:57

ehost.com.vn

ASN: AS135920

Banner

```
3.org/1999/xhtml" lang="en">

nt-type" content="text/html; charset=utf-8">

script" src="./en/welcomeRes.js"> </script>
script" src="./scripts/setUserLocale.js"> </script>
script">document.write("<title>" + ID_VC_Welcome + "</title>");</script>

href="./default.css" type="text/css" />
href="./print.css" type="text/css" media="print" />
" content="VMware vSphere is virtual infrastructure software for partitic


rc="./header-logo.png" width="586" height="42" alt="VMware vSphere 6" /><
ted">
```

SEARCH TYPE

Devices	40,896 ▾
Ipv4	40,885
Ipv6	11
Websites	37

YEAR

2021	15,881
2020	7,019

Figure 6: ZoomEye vCenter server search - unregistered (dd June 4, 2021)

Reasons for Concern

Both vulnerabilities are weaponized and exploited in the wild by malicious actors. Actors have access to a multitude of resources to perform the assessment of exposed servers and abuse them. Most important threats faced by vulnerable and exposed VMWare vCenter servers are:

- Cryptojacking: malicious cryptomining by cybercriminals on compromised servers
- Ransomware: unground actors will be leveraging the vulnerability to establish initial access and sell the foothold to crime syndicates to run their extortion campaigns
- Compromised servers are great hosts for malicious services such as Command and Control servers, spam and malicious activity relays and proxies. Hosts inside the network of legitimate organizations are harder to take down through simple blocklisting or filing abuse.
- Servers inside the data center are perfect jump hosts for lateral movement inside the network and can be leveraged for stealing and espionage

Protection And Mitigation

Radware DefensePro already protects your network against exploitation of CVE-2021-21972 with signature ID 19948. Radware is in the process of QA testing a signature to protect against exploitation of CVE 2021-21985 that will be included automatically in a next signature update.

Mass Scanning For VMWare vCenter RCE

Weaponized exploits and mass scanning activity for two critical vCenter vulnerabilities

JUNE 7, 2021

Radware's web application firewall detects and blocks potential exploits leveraging CVE-2021-21972 and CVE-2021-21985 as Code Injection violations.

Patching vCenter is still the recommended way to mitigate potential attacks. If that is not possible within an acceptable timeframe, the impacted vCenter plugins can be individually disabled. More information on disabling the plugins can be found in the VMWare knowledgebase article "How to Disable VMware Plugins in vCenter Server (83829)."

If you need vCenter servers accessible to the internet, consider not directly exposing them but rather using a VPN to limit access to trusted parties only.

Even if your vCenter servers are not exposed to the internet, you should plan to upgrade or implement the workaround as soon as possible. Internal vCenter servers can be abused for lateral movement or privilege escalation.

Indicators of Compromise (IOC)

CVE-2021-21972

Exploit detection: POST /ui/vropspluginui/rest/services/uploadova

Scanning activity: Request uri = /ui/vropspluginui/*

CVE-2021-21985

Exploit detection: POST /ui/h5-vsan/rest/proxy/service/&vsanProviderUtils_setVmodlHelper/setTargetObject

Scanning activity: Request uri = /ui/h5-vsan/rest/proxy/

EFFECTIVE DDOS PROTECTION ESSENTIALS

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

LEARN MORE AT DDOS WARRIORS

To know more about today’s attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit Radware's **Security Research Center.** It is the ultimate resource for everything security professionals need to know about DDoS attacks and cybersecurity.