NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

December 2020, Edition 1.0

NETWORK INTELLIGENCE SECURITY ADVISORY

The major security news items of the month - major threats and security patch advisory. The advisory also includes IOCs and remediation steps.

IN THIS EDITION:

Security Advisory Listing	Severity
SolarWinds Inc. an American company that develops enterprise software to assist businesses with managing entire IT infrastructure, suffered a massive security breach compromising client data	Critical
Microsoft Patch Tuesday – December 2020	Critical
FireEye, a global cyber security provider suffered a security breach by highly skilled and sophisticated state-sponsored threat actors	Critical
A Command Injection vulnerability (CVE-2020-4006) in multiple VMware products, was widely exploited by Russian-state actors	High

ALSO INSIDE

Security Patch Advisory

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

SolarWinds Inc. an American company that develops enterprise software to assist businesses with managing entire IT infrastructure, suffered a massive security breach compromising client data

Severity: Critical

Date: December 18, 2020

REMEDIATION

Immediately upgrade Orion Platform v2020.2 (with no hotfix) or 2020.2 HF 1, to latest Orion Platform version 2020.2.1 HF 2.

2. Immediately update Orion Platform v2019.4 HF 5, to latest Orion Platform version 2019.4 HF 6.

3. Ensure proper network segmentation are done, and ensure communication through TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are explicitly allowed on-demand only for particular network segments when needed.

4. Ensure network segments that allows communication over TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are strictly monitored for any anomaly or suspicious patterns like lateral movement, excessive network traffics on TCP Port 135, TCP Port 445, TCP Port 1900, TCP Port 3389, and unusual amount of data transmission, etc.

5. Ensure Domain Accounts follows least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.

6. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel.

7. Ensure VPN client software and VPN servers are patched with latest security updates released by vendor.

8. Strictly ensure TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are not left open on Internet or DMZ facing side.

9. Please ensure TCP Port 135, TCP Port 445, TCP Port1900, and TCP Port 3389, are only accessible through VPN tunnel between VPN clients and Organization's Resources.

INCIDENT BRIEFING

SolarWinds Inc. an American company that develops software for businesses to assist with managing entire IT infrastructure, has suffered security breach which impacted hundreds of customers on global scale via supply chain attack that involved wide distribution of SUNBURST backdoor through highly obfuscated update packages for SolarWinds Orion (IT monitoring and management) software.

The backdoor was hidden inside SolarWinds.Orion.Core.BusinessLayer.dll file of the SolarWinds Orion software framework, and capable of transferring files, executing files, profiling the system, rebooting the machine, and disabling system services. The backdoor communicates to C2 domains via HTTP GET and HTTP POST request methods, by masquerading its network traffic as legitimate SolarWinds activity through the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files.

The moment weaponized update packages for SolarWinds Orion software (versions v2020.2 with no hotfix and 2020.2 HF 1) is pushed to customer side and installed, the malicious SolarWinds.Orion.Core.BusinessLayer.dll file will be loaded by the legitimate SolarWinds.BusinessLayerHost.exe or SolarWinds.BusinessLayerHostx64.exe (depending on Windows system architecture). Soon after a week or two, the backdoor will attempt to resolve to multiple random subdomains of avsvmcloud[.]com.

The remote attacker with initial access onto the system via the backdoor, attempts to deploy the malware called TEARDROP (that runs as a service within the memory of the system) to hold persistence, and further install Cobalt-Strike payload called BEACON to do lateral movement from initial compromise system to other systems across enterprise-wide network.

The company SolarWinds Inc. confirmed that the supply chain attack was a manually effort, which means attackers already had initial access onto the target software update server, prior to replacing the legitimate update packages with weaponized version of update packages for SolarWinds Orion software.

It is yet unclear how remote attackers managed to gain unauthorized access onto the IT infrastructure of the SolarWinds Inc. company.

However, our Threat Intelligence team at Network Intelligence (I) Pvt Ltd., have reviewed the supply chain attack case of the SolarWinds Inc. company, and they said that the attackers behind the security breach may have taken advantage of vulnerabilities in Palo Alto GlobalProtect Gateway (CVE-2020-2050) and Palo Alto Networks PAN-OS software (CVE-2020-2000), to gain initial footholds onto the network (A) that has access to FTP File Server, SolarWinds software installer packages, internal remote support system, and Cisco Expressway E. The attackers might have used cobalt-strike beacon to gain further access onto the adjacent network (B) that hosts ADFS Single SignOn (SSO) service for SolarWinds Service Desk account, and Bitbucket repository service. Maybe with help of SSO account credentials, attackers might have wider access across the cloud infrastructures of SolarWinds Inc. company.

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

SolarWinds Inc. an American company that develops enterprise software to assist businesses with managing entire IT infrastructure, suffered a massive security breach compromising client data

Severity: Critical

Date: December 18, 2020

REMEDIATION

10. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).

11. Ensure to monitor for excessive LDAP queries within 5 minutes from particular system, via SIEM solution.

12. Ensure VNC, SOCKS, and SMTP ports are also closelymonitored.

13. Ensure data backup is done periodically and ensure data backups are done via out-of-band network onto the server with limited or no internet access.

14. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

15. Ensure to create and enable detection based on Yara, Snort, ClamAV, and HXIOC rules from FireEye.

IP ADDRESS

96.31.172.122
96.31.172.115
96.31.172.202
96.31.172.135
96.31.172.155
96.31.172.30
96.31.172.125
96.31.172.227
20.140.0.1
20.140.194.200
20.140.201.185
20.141.141.240
20.141.233.31
20.140.99.218
20.140.211.243
20.141.184.161
204.188.205.176
167.114.213.199
18.217.225.111
13.57.184.217
3.16.81.254
34.219.234.134
3.87.182.149
196.203.11.89
18.220.219.143
5.252.177.21
139.99.115.204
13.59.205.66
34.203.203.23
54.215.192.52
5.252.177.25
54.193.127.66
51.89.125.18

INCIDENT BRIEFING

Our Threat Intelligence team added that the attackers (equivalent to APT or Nation-state) often target vulnerabilities and misconfiguration issues in solutions such as Single Sign-On (SSO), Identity Access Management (IAM), Privilege Access Management (PAM), Virtual Private Network (VPN), and Web Application Firewall (WAF) hosted on cloud or on-premise IT Infrastructure. So, its very important to keep track on vulnerabilities disclosed by technology vendors and apply security patches when released.

Our Threat Intelligence team further added that the current threat landscape is getting increasingly worst each day, since attackers irrespective of their end goals are leveraging cobalt-strike tools in their attack chain, and this has become quite common trend in malware and hacking campaigns since August 2020. It is strongly recommended to adopt and implement zero-trust model across enterprise-wide cyber security operations and management. And, ensure to block below Indicators of Compromise (IOCs).

DOMAINS

lcomputers.com
kubecloud.com
webcodez.com
solartrackingsystem.net
avsvmcloud.com
seobundlekit.com
digitalcollege.org
globalnetworkissues.com
websitetheme.com
freescanonline.com
virtualwebdata.com
virtualdataserver.com
databasegalore.com
panhardware.com
thedoccloud.com
highdatabase.com
deftsecurity.com
zupertech.com
incomeupdate.com

SUBDOMAINS

ahmad-test.avsvmcloud.com
earn.avsvmcloud.com
108-62.avsvmcloud.com
eu-west-i.avsvmcloud.com
scl.avsvmcloud.com
106-63.avsvmcloud.com
fa2.avsvmcloud.com
15e65.avsvmcloud.com
8-8.avsvmcloud.com
3bnat.avsvmcloud.com
tbe.avsvmcloud.com
15e9c.avsvmcloud.com
10782.avsvmcloud.com
32131.avsvmcloud.com
26f6.avsvmcloud.com
707.avsvmcloud.com
kenl.avsvmcloud.com
testfrombrowser.avsvmcloud.com
28310.avsvmcloud.com
2782.avsvmcloud.com
roos.avsvmcloud.com
u2.avsvmcloud.com
wf.avsvmcloud.com
best.avsvmcloud.com
110-133.avsvmcloud.com
hrh.avsvmcloud.com
18.avsvmcloud.com
bn.avsvmcloud.com
mn.avsvmcloud.com
4.avsvmcloud.com
kia.avsvmcloud.com
sol.avsvmcloud.com
amb.avsvmcloud.com

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

SolarWinds Inc. an American company that develops enterprise software to assist businesses with managing entire IT infrastructure, suffered a massive security breach compromising client data

Severity: Critical

Date: December 18, 2020

SUBDOMAINS

mcm.avsvmcloud.com
cm.avsvmcloud.com
66.avsvmcloud.com
sim.avsvmcloud.com
vpn.avsvmcloud.com
trail.avsvmcloud.com
jmak.avsvmcloud.com
p111.avsvmcloud.com
btb.avsvmcloud.com
103-157.avsvmcloud.com
1-232.avsvmcloud.com
100-194.avsvmcloud.com
woe.avsvmcloud.com
2d8f5.avsvmcloud.com
9b8.avsvmcloud.com
eze.avsvmcloud.com
1eec.avsvmcloud.com
12742.avsvmcloud.com
13f4c.avsvmcloud.com
10-177.avsvmcloud.com
engn.avsvmcloud.com
joc.avsvmcloud.com
713.avsvmcloud.com
reve.avsvmcloud.com
ivc.avsvmcloud.com
1-136.avsvmcloud.com
rid.avsvmcloud.com
37-78.avsvmcloud.com
100000000www.avsvmcloud.com
1c210.avsvmcloud.com
a6.avsvmcloud.com
buz.avsvmcloud.com
f6.avsvmcloud.com
cil.avsvmcloud.com
115933.avsvmcloud.com
10f8a.avsvmcloud.com
iic.avsvmcloud.com
114zuqiudaohang.avsvmcloud.com
adp.avsvmcloud.com
pcpc.avsvmcloud.com
x231.avsvmcloud.com
ft.avsvmcloud.com
dn76.avsvmcloud.com
2d95f.avsvmcloud.com
32d.avsvmcloud.com
gi2j.avsvmcloud.com
gtp.avsvmcloud.com
pm3.avsvmcloud.com
czen.avsvmcloud.com
m94.avsvmcloud.com
jh.avsvmcloud.com
39557.avsvmcloud.com
ape.avsvmcloud.com
106-210.avsvmcloud.com
p2.avsvmcloud.com
36188.avsvmcloud.com

SUBDOMAINS

t15.avsvmcloud.com
1599.avsvmcloud.com
5bc.avsvmcloud.com
sii.avsvmcloud.com
10265.avsvmcloud.com
113-148.avsvmcloud.com
899.avsvmcloud.com
89a.avsvmcloud.com
370.avsvmcloud.com
23341.avsvmcloud.com
c-api.us-east-2.avsvmcloud.com

HASHES (SHA-256)

d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
abe22cf0d78836c3ea072daeaf4c5eeaf9c29b6feb597741651979fc8fbd2417
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af
292327e5c94afa352cc5a02ca273df543f2020d0e76368ff96c84f4e90778712
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71
53f8dfc65169ccda021b72a62e0c22a4db7c4077f002fa742717d41b3c40f2c7
439bcd0a17d53837bc29fb51c0abd9d52a747227f97133f8ad794d9cc0ef191e
69f998bd67a5dbfd79bcc44f0cf2284ed61fac9bfaba3d3b4dfb19a57baa29c5
11ae7e7ab4d36dfe0bc33fd7719eaea5acd0ecbe17b32943660acb7647c33c34
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
e9fff8e51a463e60e55a00732b3d5fcd423a86537d8d8c306d1cf7022e885fa8
b8d64f7695aa98cea1c8a8bdc9fc8cbf7a12217164036216ecf44f964ac625f3
d9e08400ef4679ea08ad5bbc64adafc700c6bef81ae396e4d93c1851a93f2105
2ffa8d2de81240fae48b4b7819f41b7f8dcbef6eec597d59c48401aa68e24944
2bb8d5b8428113788a23fd57b0d92612f0b67aaa1e1c5556d63ab805b50a08bc
7c2b3f464200835f0a4cc80f7202fbe72291cdaad01d9909c6b16f4469ef9a9c
d47dcf7722a6b61d0ca9679aa46a471b45cf8a27218632547c9b474999bdc8c7
70b85bdfa4cde280dd34712f74ae3b588efe891fd3444dd1cfa9c1c71810a93a
467a4d4cd4cad073fb04a22cf923c05792ed9618fed11a072c55487cacfec592
71cd6b925a864ccfea2564fb4c715790e170777d041e22902f0f2369e9f8ed67
c7e38d407c1cc91faf8721631aa7b7bb7a0afc2a2cb32c87d10aa5d7e1aa9451

URL

https<://>downloads.solarwinds.com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20574/SolarWinds-Core-v2019.4.5220-Hotfix5.msp

Reference

- Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor
- SolarWinds Security Advisory

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Microsoft Patch Tuesday – December 2020

Severity: Critical

Date: December 10, 2020

IMPACT

On successful exploitation of these vulnerabilities would allow remote attacker to execute malicious code in context of user account and take ownership of the affected Microsoft Products.

REMEDIATION

1. Kindly apply available Microsoft patches on Microsoft Windows Workstations & Servers.

2. Kindly refer Server Products, Workstation Products and Application Products Tabs in attached Excel Sheet, to prioritize patch and patch management process for critical IT assets.

INTRODUCTION

Microsoft released security patches for 58 vulnerabilities in various Microsoft products such as Windows Workstations & Servers, Exchange, SharePoint and Office, which would allow unauthenticated remote attacker to execute malicious code in the context of user account.

And also, Microsoft released security patches for very critical vulnerabilities (CVE-2020-17095, CVE-2020-17096, and CVE-2020-17099) in Microsoft Windows Workstation and Server products, that are more likely to be exploited in targeted malware or ransomware attacks and hacking campaigns.

IMPORTANT

Microsoft Windows 10 1903 Pro, Pro Education, Pro for Workstations, Enterprise, and IoT Enterprise, is reaching end of service on December 8th, 2020.

Microsoft Windows 10 1803 Enterprise, IoT Enterprise, and education users get an extra year of servicing, with their end of support being May 11th, 2021.

Microsoft Windows 10 1803 Pro, Pro for Workstation, and IoT Core has reached end of support on November 12th, 2019, as well as Microsoft Windows 7 has reached end of support on January 14th, 2020, which means they will no longer receive security updates and will be vulnerable to any new security threats that are discovered. We recommend upgrading to latest supported versions of Microsoft Windows OS

AFFECTED PRODUCTS

- Microsoft Windows Workstation and Server products.
- Microsoft Visual Studio, Azure, Exchange, and SharePoint
- Servers products.
- Microsoft Edge, and Office products

READ

- December 2020 Security Updates
- Microsoft December 2020 Patch Tuesday fixes 58 vulnerabilities

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

FireEye, a global cyber security provider suffered a security breach by highly skilled and sophisticated state-sponsored threat actors

Severity: Critical

Date: December 09, 2020

REMEDIATION

Ensure Microsoft Windows Server, Microsoft SharePoint Server, Microsoft Exchange Server, and Microsoft IIS Server, are patched with latest security updates.

2. Ensure proper network segmentation are done, and ensure communication through TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are explicitly allowed on-demand only for particular network segments when needed.

3. Ensure network segments that allowscommunication over TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389 are strictlymonitored for any anomaly or suspicious patterns like lateral movement, excessive network trafficson TCP Port 135, TCP Port 445, TCP Port 1900, TCPPort 3389, and unusual amount of data transmission, etc.

4. Ensure Domain Accounts follows least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.

5. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel.

6. Ensure VPN client software and VPN servers are patched with latest security updates released by vendor.

7. Strictly ensure TCP Port 135, TCP Port 445, TCP Port1900, and TCP Port 3389 are not left open on Internet or DMZ facing side.

8. Please ensure TCP Port 135, TCP Port 445, TCP Port 1900, and TCP Port 3389, are only accessible through VPN tunnel between VPN clients and Organization's Resources.

9. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).

INCIDENT BRIEFING

FireEye, a global cybersecurity company suffered security breach by highly skilled and sophisticated nation-state threat actors.

The nation-state threat actors behind the attack were managed to steal Red Team Assessment Tools of FireEye company, that were used to evaluate security controls for their customers from diverse industries including Government and Defence organizations, Aerospace and Aviation, Energy Sectors, and many others.

The nation-state threat actors are believed to be well trained in operational security and executed the attack with discipline and precise focus on stealing sensitive data.

For the first time in last 25 years in cyber security and incident response, FireEye witnessed this highly sophisticated attack by nation-state threat actors at first hand, with no prior knowledge or evidence about the attack.

The nation-state threat actors used a novel combination of techniques to counter security tools and forensic examination, which prevented FireEye from detecting and investigating the intrusion while it was in-progress.

FireEye is actively investigating the security breach incident with help of Federal Bureau of Investigation (FBI) and other key partners, including Microsoft.

FireEye however, managed to release files hashes of stolen Red Team Assessment Tools, and also released detection rules in Yara, Snort, ClamAV, and HXIOC.

REMEDIATION

10. Ensure to monitor for excessive LDAP queries within 5 minutes from particular system, via SIEM solution.

11. Ensure VNC, SOCKS, and SMTP ports are also closely monitored.

12. Ensure data backup is done periodically and ensure data backups are done via out-of-band network onto the server with limited or no internet access.

13. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

14. Ensure to create and enable detection based on Yara, Snort, ClamAV, and HXIOC rules from FireEye.

READ

- FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community
- Unauthorized Access of FireEye Red Team Tools
- FireEye Cyberattack Compromises Red-Team Security Tools
- Top cybersecurity firm FireEye hacked by a nation-state actor
- FireEye Red Team Tool Countermeasures

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

FireEye, a global cyber security provider suffered a security breach by highly skilled and sophisticated state-sponsored threat actors

Severity: Critical

Date: December 09, 2020

HASH (SHA-256)

Hashes	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
0340043481091d92dcfb2c498aad3c0a fca2fd208ef896f65af790cc147f8891	Yes	Yes	yes	Yes	Yes
078403b4e89ff06d2fe2ed7e75428a38 1f83ffb708dbd01b0220767498947f0c	Yes	No	Yes	No	Yes
b6ef03aec5d10e371f0b06c661036d838 ef55fa7dc75cf91fca3622bdefa8140	Yes	Yes	yes	Yes	Yes
1cf5710e500a423b84b51fa3afdd923fe 0a8255c5817d3238175623e2ebbfad9	Yes	Yes	Yes	No	Yes
82cce26c60a5105e6caf5ac92eabb3ded cd883cd075f2056f27b0ec58aefaaa6	Yes	Yes	Yes	No	Yes
c0621954bd329b5cabe45e92b310536 27c27fa40853beb2cce2734fa677ffd93	Yes	Yes	Yes	Yes	Yes
a022820a62198fa3e3b89749b38db1cc3a09 136524682fb99a3ce36652725065	No	No	Yes	No	No
efb533249f71ea6ebfb6418bb67c94e8f bd5f2a26cbd82ef8ec1d30c0c90c6c1	No	No	Yes	No	No
d9882283ee2dc487c2a5fb97f8067051 c259c4721cd4aea8c435302fe6b274c4	Yes	Yes	Yes	No	Yes
25e755c8957163376b3437ce808843c1 c2598e0fb3c5f31dc958576cd5cde63e	Yes	Yes	Yes	Yes	Yes
69f998bd67a5dbfd79bcc44f0cf2284ed6 1fac9bfaba3d3b4dfb19a57baa29c5	Yes	No	Yes	Yes	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

FireEye, a global cyber security provider suffered a security breach by highly skilled and sophisticated state-sponsored threat actors

Severity: Critical

Date: December 09, 2020

HASHES (MD5)

Hashes	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
f41074be5b423afb02a74bc74222e35d	Not Known	Not Known	Not Known	Not Known	Not Known
e89efa88e3fda86be48c0cc8f2ef7230	Not Known	Not Known	Not Known	Not Known	Not Known
995120b35db9d2f36d7d0ae0bfc9c10d	Not Known	Not Known	Not Known	Not Known	Not Known
f7d9961463b5110a3d70ee2e97842ed3	Not Known	Not Known	Not Known	Not Known	Not Known
f20824fa6e5c81e3804419f108445368	Not Known	Not Known	Not Known	Not Known	Not Known
5e14f77f85fd9a5be46e7f04b8a144f5	Not Known	Not Known	Not Known	Not Known	Not Known
dd8805d0e470e59b829d98397507d8c2	Not Known	Not Known	Not Known	Not Known	Not Known
7af24305a409a2b8f83ece27bb0f7900	Not Known	Not Known	Not Known	Not Known	Not Known
100d73b35f23b2fe84bf7cd37140bf4d	Not Known	Not Known	Not Known	Not Known	Not Known
4e7e90c7147ee8aa01275894734f4492	Not Known	Not Known	Not Known	Not Known	Not Known
edcd58ba5b1b87705e95089002312281	Not Known	Not Known	Not Known	Not Known	Not Known

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A Command Injection vulnerability (CVE-2020-4006) in multiple VMware products, was widely exploited by Russian-state actors

Severity: High

Date: December 08, 2020

IMPACT

This vulnerability poses a severe risk of unauthorized access, data breach, security breach, disruption in business operation, financial losses, and impact reputation of an organization.

REMEDIATION

1. Kindly apply security patches for VMware Workspace ONE Access versions 20.10, and 20.01.

2. Kindly apply security patches for VMware Identity Manager versions 19.03, and 19.03.0.1.

3. Kindly apply security patches for VMware Identity Manager versions 3.3.3, 3.3.2, and 3.3.1.

WORKAROUND

For temporary workaround, please refer to the instructions mentioned in Solution section of the VMware Knowledgebase Article 81731

INTRODUCTION

A Command Injection vulnerability (CVE-2020-4006) in multiple VMware products, is widely exploited by Russian nation-state actors.

Threat Actors behind the hacking campaign are more focused on stealing sensitive data by abusing a vulnerability in VMware products such as VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector.
To exploit this vulnerability, the threat actors must have valid admin credential and initial access to corporate network. This can only be achieved through spear-phishing email sent to privileged users, asking for login credential, or intended to deliver malware to seek initial access onto the system and then steal login credential prior to exploiting the vulnerability and proceed to cause further damages such as data breach, and ransomware attack for instance.

This vulnerability poses a severe risk of unauthorized access, data breach, security breach, disruption in business operation, financial losses, and impact reputation of an organization.

AFFECTED PRODUCTS

- VMware Workspace One Access (Access) 20.10 and 20.01
- VMware Workspace One Access Connector (Access Connector) 20.10, 20.01.0.0, and 20.01.0.1
- VMware Identity Manager (vIDM) 3.3.3, 3.3.2, and 3.3.1
- VMware Identity Manager Connector (vIDM Connector)
- 19.03.0.0, 19.03.0.1, 3.3.3, 3.3.2, and 3.3.1

READ

- HW-128524: CVE-2020-4006 for Workspace ONE Access, Identity Manager and Connector (81754)
- Russian State-Sponsored Malicious Cyber Actors Exploit Known Vulnerability in Virtual Workspaces
- Russia-linked hackers actively exploit CVE-2020-4006 VMware flaw, NSA warns

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

14th December 2020 – 20th December 2020 | TRAC-ID: NII20.12.0.3

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
December 16, 2020	Ubuntu Linux	USN-4672-1: unzip vulnerabilities	▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS ▪ Ubuntu 14.04 ESM ▪ Ubuntu 12.04 ESM	Security Patch Update
December 15, 2020	Ubuntu Linux	USN-4671-1: Firefox vulnerabilities	▪ Ubuntu 20.10 ▪ Ubuntu 20.04 LTS ▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS	Security Patch Update
December 15, 2020	Ubuntu Linux	USN-4670-1: ImageMagick vulnerabilities	▪ Ubuntu 20.10 ▪ Ubuntu 20.04 LTS ▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS	Security Patch Update

REDHAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
December 17, 2020	Red Hat Single Sign-On	RHSA-2020:5625	▪ Red Hat Single Sign-On Text-Only Advisories x86_64	Security Patch Update
December 17, 2020	Red Hat Enterprise Linux	RHSA-2020:5618	▪ Red Hat Enterprise Linux Server 7 x86_64 ▪ Red Hat Enterprise Linux Workstation 7 x86_64 ▪ Red Hat Enterprise Linux Desktop 7 x86_64	Security Patch Update

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

14th December 2020 – 20th December 2020 | TRAC-ID: NII20.12.0.3

December 16, 2020	**Red Hat Enterprise Linux**	**RHSA-2020:5566**	▪ Red Hat Enterprise Linux Server 7 x86_64 ▪ Red Hat Enterprise Linux Workstation 7 x86_64 ▪ Red Hat Enterprise Linux Desktop 7 x86_64	**Security Patch Update**
December 16, 2020	**Red Hat Enterprise Linux**	**RHSA-2020:5561**	▪ Red Hat Enterprise Linux Server 7 x86_64 ▪ Red Hat Enterprise Linux Workstation 7 x86_64 ▪ Red Hat Enterprise Linux Desktop 7 x86_64	**Security Patch Update**

IBM

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
December 18, 2020	**IBM QM**	**IBM MQ could allow an authenticated user, under nondefault configuration to cause a data corruption attack due to an error when using segmented messages. (CVE-2020-4592)**	▪ IBM MQ 9.1 LTS ▪ IBM MQ 9.0 LTS ▪ IBM MQ 8.0 ▪ IBM MQ 9.1 CD ▪ IBM MQ 7.5	**Kindly update to fixed version**
December 18, 2020	**IBM AIX and IBM VIOS**	**Vulnerability in BIND affects AIX (CVE-2020-8622)**	▪ AIX 7.1 ▪ AIX 7.2 ▪ VIOS 3.1	**Kindly update to fixed version**