NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

September 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
Rampant Kitten, an Iranian APT threat actor, was found to be targeting Government and Defence Organizations using various attack vectors and customized Malware	High
Remote Code Execution vulnerability (CVE-2020-16875) in Microsoft Exchange Server, and Elevation of Privilege vulnerability (CVE-2020-1472) in Microsoft Windows Server were found to be exploited	Critical
Microsoft September 2020 Patch Tuesday fixed 23 critical vulnerabilities which included security patches for vulnerabilities (CVE-2020-0837, CVE-2020-0839, CVE-2020-0912, CVE-2020-1030, and CVE-2020-1598) in Microsoft Server products were widely exploited in targeted malware attacks and hacking campaigns	Critical
Threat Actors were found to be targeting State Government Organizations in Middle East and North Africa using Thanos Ransomware that overwrote MBR to prevent system bootup	Critical
The Memory Exhaustion Vulnerabilities (CVE-2020-3566 and CVE-2020-3569) in DVMRP feature of Cisco IOS XR Software were found to be exploited in targeted Hacking Campaigns and Malware Attacks	High
TA505 Threat Actors were found cybersquatting domains of popular brands including PayPal, Google, Microsoft, etc. for committing financial and consumer frauds	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

Rampant Kitten, an Iranian APT threat actor, was found to be targeting Government and Defence Organizations using various attack vectors and customized Malware

Severity: High

Date: September 23, 2020

IP ADDRESSES

148.251.97.102
176.31.4.14
148.251.224.29
144.76.177.244
137.74.153.98

DOMAIN

telegramreport.me
telegramco.org
telegrambots.me
mailgoogle.info
gradleservice.info
alarabiye.net
afalr-sharepoint.com
afalr-onedrive.com
exemplifiable-taps.000webhostapp.com
telegramup.com
tbackup.000webhostapp.com
vareangold.de
telegrambackups.com
telegramdesktop.com
picfile.net
developerchrome.com
firefox-addons.com
cpuconfig.com
update-help.com
winchecking.com
endupload.com

REMEDIATION

1. Immediately apply Security Patches for Microsoft vulnerabilities CVE-2020- 0837, CVE-2020-0839, CVE-2020-0912, CVE-2020-1030, & CVE-2020-1598 on Microsoft Windows Workstation and Server.
2. Ensure Microsoft Windows Servers are patched with latest security updates.
3. Ensure Domain Accounts follows least privilege principle and ensure TwoFactor authentication is enabled on all Business Email Accounts.
4. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel.
5. Ensure VPN client software and VPN servers are patched with latest security updates released by vendor.
6. Strictly ensure TCP Port 135, TCP Port 445, and TCP Port 3389 are not left open on Internet or DMZ facing side.
7. Please ensure TCP Port 135 (Remote Procedure Call - RPC), TCP Port 445 (Server Message Block - SMB), and TCP Port 3389 (Remote Desktop Protocol - RDP) are only accessible through VPN tunnel between VPN clients and Organization's Resources.
8. Ensure proper network segmentation are done, and ensure communication through TCP Port 135, TCP Port 445, and TCP Port 3389 are explicitly allowed on-demand only for particular network segments when needed.
9. Ensure network segments that allows communication over TCP Port 135, TCP Port 445, 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 3389, and unusual amount of data transmission, etc.
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 closely monitored.
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 IPs and Domains on the perimeter security devices.
15. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

READ

- Rampant Kitten – An Iranian Espionage Campaign

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Rampant Kitten, an Iranian APT threat actor, was found to be targeting Government and Defence Organizations using various attack vectors and customized Malware

Severity: High

Date: September 23, 2020

HASHES (MD5)

HASHES	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
4415e6240b037f4ac693c7e4a88f5ab2567b68dddbaa8fbfb0b40d37748fa8ba	Yes	Yes	Yes	No	Yes
2c4156bb1d1e3f0abafd5d03fad277f6aab705cb917bc07e05de3170fd80854f	Yes	Yes	Yes	No	Yes
69cbda8c2ea92eace49d678cc660432d0ad0c44bd79c3a02dd841066f80bc51b	Not Known	Not Known	Not Known	Not Known	Not Known
525e99feb0a32a96aaf6e34be899e6a68c7abb6a8542f30e3822d07fe4e8d278	Not Known	Not Known	Not Known	Not Known	Not Known
54a20f35d302499c925e5855f782bacb6bdd0a345f57c9e80772ef29fb81f465	Not Known	Not Known	Not Known	Not Known	Not Known
083fe2c0feca89a6011ea2749123e216e0a53b573ebef2f25d856412cee7f99c	Not Known	Not Known	Not Known	Not Known	Not Known
51a9a7e764a509b979dd438719840369718a320acbba32abbf51d4926e7d3486	Not Known	Not Known	Not Known	Not Known	Not Known
b7730f9a05be8a0f25a3979b2f8d2fed791340a32385a9fd37d0e8b81119627d	Yes	Yes	Yes	No	Yes
63a655fde88ea26c73cea1e1764305e44203db771f64155b3b3e3d805203f65a	Yes	Yes	Yes	No	Yes
5eb4c94c9927e90426b6227754ae97fca06d468d5512d15773c48817ea082dbf	Yes	Yes	Yes	No	Yes
dff78dc100c1efd116de1a1d9e0b9169380801a1e7e864d63dc81a263f8929e8	Yes	Yes	Yes	No	Yes
845a0e5720a6288794a6452adb8d3e7c22f5e6e6b9d4f7481fbd30e3efba4f28	Yes	Yes	Yes	Yes	Yes
b7437e3d5ca22484a13cae19bf805983a2e9471b34853d95b67d4215ec30a00e	No	No	No	No	No
0e4a8eb2fe861c45071626da24147e922b167efb543e37ace7466c74c1e98be6	No	Yes	Yes	No	Yes
0f7082926241659fbebd229cdc41abe358be49110a80729b9ee891f2f7dcdf16	Yes	Yes	Yes	No	Yes
71085b661fea6cf040586b462b07ce8e0471fb9208c4f69cfd168e168beab6fe	Yes	Yes	Yes	No	Yes
37f40214d2f150597c52cb868c1e2f723d9c2d3155ab18ab2f1279eaf09bdf71	Yes	Yes	Yes	Yes	Yes
f211a92c2e215c2691006407bc919a892dd998120d83d333f2295059cd3c1c60	Yes	Yes	Yes	Yes	Yes
1b8cd7c93dce63878dadae0cf77482ae367477841a4604c6a842158466790737	Yes	Yes	Yes	Yes	Yes
d148562a49a09333b2b02d13e12b183d4c3fcf23fbb024d4e0b440631a3a3663	Yes	Yes	Yes	No	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Remote Code Execution vulnerability (CVE-2020-16875) in Microsoft Exchange Server, and Elevation of Privilege vulnerability (CVE-2020-1472) in Microsoft Windows Server were found to be exploited

Severity: Critical

Date: September 22, 2020

IMPACT

On successful exploitation of these vulnerabilities would allow unauthenticated remote attacker to gain unauthorized access and cause data breach.

REMEDIATION

1. Immediately apply security patches for vulnerability (CVE-2020-16875) in Microsoft Exchange Server, and for vulnerability (CVE-2020-1472) in Microsoft Windows Server.

(Please refer attached Excel Sheet for quick access to Security Patches)

INTRODUCTION

Remote Code Execution vulnerability (CVE-2020-16875) in Microsoft Exchange Server, and Elevation of Privilege vulnerability (CVE-2020-1472) in Microsoft Windows Server are found exploited in wide.

Attackers are taking advantage of these two vulnerabilities in targeted Malware Attacks and Hacking Campaigns.

The vulnerability (CVE-2020-16875) in Microsoft Exchange Server is due to improper validation of cmdlet arguments that allows authenticated remote attacker with user credential (having access to certain Exchange role), to execute arbitrary code in the context of the System user.

Whereas, the vulnerability (CVE-2020-1472) in Microsoft Windows Server is due to Netlogon Remote Protocol establishes a vulnerable Netlogon secure channel connection to a domain controller, that allows unauthenticated remote attacker to obtain domain administrator access and run a specially crafted application on a device on the network.

Microsoft has partially addressed this vulnerability (CVE-2020-1472) by modifying how Netlogon handles the usage of Netlogon secure channels, but Microsoft will soon release another security patch to completely fix this vulnerability during Q1 2021.

These vulnerabilities pose a severe risk of unauthorized access and data breach incident. We strongly recommend our customers to immediately patch these vulnerabilities on Microsoft Exchange and Microsoft Windows Servers.

AFFECTED PRODUCTS

• Microsoft Exchange Server 2016 Cumulative Update 16 and 17
• Microsoft Exchange Server 2019 Cumulative Update 5 and 6
• Windows Server 2008 R2 for x64-based Systems Service Pack 1 and Server Core installation
• Windows Server 2012 and Server Core installation
• Windows Server 2012 R2 and Server Core installation
• Windows Server 2016 and Server Core installation
• Windows Server 2019 and Server Core installation
• Windows Server version 1903 (Server Core installation)
• Windows Server version 1909 (Server Core installation)
• Windows Server version 2004 (Server Core installation)

READ

- CVE-2020-16875 | Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability
- How to manage the changes in Netlogon secure channel connections associated with CVE- 2020-14

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Microsoft September 2020 Patch Tuesday fixed 23 critical vulnerabilities which included security patches for vulnerabilities (CVE-2020-0837, CVE-2020-0839, CVE-2020-0912, CVE-2020-1030, and CVE-2020-1598) in Microsoft Server products were widely exploited in targeted malware attacks and hacking campaigns

Severity: Critical

Date: September 09, 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

EXPLOITABLE CVE IDs

Kindly refer EXPLOITABLE CVE IDs tab in attached Excel sheet

REMEDIATION

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

2. Immediately apply security patches for products mentioned under EXPLOITABLE PRODUCTS tab in attached Excel Sheet, on Windows Servers and Workstations.

3. 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 129 vulnerabilities in various Microsoft products such as Windows Workstations & Servers, Internet Explorer Browser, 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-2020-0837, CVE-2020-0839, CVE-2020-0912, CVE-2020-1030, and CVE-2020-1598) in Microsoft Windows Workstation and Server products, that are widely exploited in targeted malware or ransomware attacks and hacking campaigns.

IMPORTANT

Microsoft Windows 10 1903 is reaching end of service on December 8th, 2020.
Microsoft delayed the end of service for several editions of Microsoft Windows 10 1803 /1809 to May 11th, 2021, due to the current public health situation.
Microsoft Windows 10 1803 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.
Microsoft Windows 10 1803 Enterprise and education users get an extra year of servicing, with their end of support being November 10th, 2020.

AFFECTED PRODUCTS

- Microsoft Windows Workstation and Server products.
- Microsoft Visual Studio, Exchange, and SharePoint Servers
- products.
- Microsoft Internet Explorer, Defender, and Office products

READ

- September 2020 Security Updates
- Microsoft September 2020 Patch Tuesday fixes 129 vulnerabilities

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Threat Actors were found to be targeting State Government Organizations in Middle East and North Africa using Thanos Ransomware that overwrote MBR to prevent system bootup

Severity: Critical

Date: September 08, 2020

IP ADDRESSES

107.174.241.175

DOMAIN

dc.services.visualstudio.com

URL

https<://>dc.services.visualstudio.com/v2/track
https<://>raw.githubusercontent.com/d35ha/ProcessHide/master/bins/ProcessHide64.exe

REMEDIATION

1. Immediately apply Security Patches for Microsoft vulnerabilities CVE-2020-1380, CVE-2020-1464, CVE-2020-1472, CVE-2020-1519, CVE-2020-1538, CVE-2020-1579, CVE-2020-1337, CVE-2020-0986, CVE-2020-0674, CVE-2019-1429, CVE-2019-0676, & CVE-2018-8653 on Microsoft Windows Workstation and Server.
2. Ensure Microsoft Windows Servers are patched with latest security updates.
3. Ensure Domain Accounts follows least privilege principle and ensure TwoFactor authentication is enabled on all Business Email Accounts.
4. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel.
5. Ensure VPN client software and VPN servers are patched with latest security updates released by vendor.
6. Strictly ensure TCP Port 135, TCP Port 445, and TCP Port 3389 are not left open on Internet or DMZ facing side.
7. Please ensure TCP Port 135 (Remote Procedure Call - RPC), TCP Port 445 (Server Message Block - SMB), and TCP Port 3389 (Remote Desktop Protocol - RDP) are only accessible through VPN tunnel between VPN clients and Organization's Resources.
8. Ensure proper network segmentation are done, and ensure communication through TCP Port 135, TCP Port 445, and TCP Port 3389 are explicitly allowed on-demand only for particular network segments when needed.
9. Ensure network segments that allows communication over TCP Port 135, TCP Port 445, 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 3389, and unusual amount of data transmission, etc.
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 closely monitored.
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 IPs and Domains on the perimeter security devices.
15. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

READ

- Thanos Ransomware: Destructive Variant Targeting State-Run Organizations in the Middle East and North Africa

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Threat Actors were found to be targeting State Government Organizations in Middle East and North Africa using Thanos Ransomware that overwrote MBR to prevent system bootup

Severity: Critical

Date: September 08, 2020

HASHES (MD5)

HASHES	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
40890a1ce7c5bf8fda7bd84b49c577e76e0431e4ce9104cc152694fc0029ccbf	Yes	Yes	Yes	No	Yes
06d5967a6b90b5b5f6a24b5f1e6bfc0fc5c82e7674817644d9c3de61008236dc	Yes	No	No	No	Yes
cbb95952001cdc3492ae8fd56701ceff1d1589bcfafd74be86991dc59385b82d	Yes	No	No	No	Yes
240e3bd7209dc5151b3ead0285e29706dff5363b527d16ebcc2548c0450db819	Yes	No	No	No	Yes
7aa46a296fbebdf3b13d399bf0dbe6e8a8fbcbc9ba696e5698326494b0da2e54	Not Known	Not Known	Not Known	Not Known	Not Known
58bfb9fa8889550d13f42473956dc2a7ec4f3abb18fd3faeaa38089d513c171f	Yes	Yes	Yes	Yes	Yes
c460fc0d4fdaf5c68623e18de106f1c3601d7bd6ba80ddad86c10fd6ea123850	Yes	Yes	Yes	Yes	Yes
ae66e009e16f0fad3b70ad20801f48f2edb904fa5341a89e126a26fd3fc80f75	Yes	No	No	No	Yes
5d40615701c48a122e44f831e7c8643d07765629a83b15d090587f469c77693d	Yes	Yes	Yes	Yes	Yes
b60e92004d394d0b14a8953a2ba29951c79f2f8a6c94f495e3153dfbbef115b6	No	No	No	No	No
dea45dd3a35a5d92efa2726b52b0275121dceafdc7717a406f4cd294b10cd67e	No	No	No	No	No
a224cbaaaf43dfeb3c4f467610073711faed8d324c81c65579f49832ee17bda8	Yes	Yes	Yes	Yes	No
b7437e3d5ca22484a13cae19bf805983a2e9471b34853d95b67d4215ec30a00e	No	No	No	No	No
ff0b7d8ca667b948c3192d85beaeffd1b99ea02f1f2a51a6e162891ee5932198	Not Known	No	Yes	Yes	Yes
647983ebde53e0501ff1af8ef6190dfeea5ccc64caf7dce808f1e3d98fb66a3c	No	No	No	No	No
6535ba91fcca7174c3974b19d9ab471f322c2bf49506ef03424517310080be1b	No	No	No	No	Not Known
6cdb16749b244d171856b02541256daa91d5fe9b7735df8b2ee3ee4cc5016d52	No	No	Yes	Yes	Yes
ea308c76a2f927b160a143d94072b0dce232e04b751f0c6432a94e05164e716d	No	No	No	No	No
1a338588919ed8caee7b195077ed6ba020971c953a8c9b6235457e0b19b18fb9	Not Known	No	Yes	No	Yes
4d0ad4d43c59dd08881b9d54ea98b15ed7cacb4e72795940e08f713907ca0643	No	No	No	No	No

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

The Memory Exhaustion Vulnerabilities (CVE-2020-3566 and CVE-2020-3569) in DVMRP feature of Cisco IOS XR Software were found to be exploited in targeted Hacking Campaigns and Malware Attacks

Severity: High

Date: September 02, 2020

IMPACT

On successful exploitation of these vulnerabilities would allow unauthenticated remote attacker to either immediately crash the Internet Group Management Protocol (IGMP) process, or cause memory exhaustion which eventually results in crash.

REMEDIATION

1. Ensure to upgrade or update Cisco IOS XR Software to latest version when available or release.

MITIGATIONS

1. As a mitigation for the memory exhaustion case, it is recommended that customers implement a rate limiter using the below command:

Router(config)# lpts pifib hardware police flow igmp rate <value>

2. As a mitigation for both the memory exhaustion case and the immediate IGMP process crash case, customers may either modify existing interface ACL or create a new ACL for specific interface that denies DVMRP traffic inbound on that interface, using the below command which creates an ACL and denies DVMRP traffic:

Router(config)# ipv4 access-list <acl_name> deny igmp any any dvmrp

INTRODUCTION

The Memory Exhaustion Vulnerabilities (CVE-2020-3566 and CVE-2020-3569) in Distance Vector Multicast Routing Protocol (DVMRP) feature of Cisco IOS XR Software, found widely exploited in targeted Hacking Campaigns and Malware Attacks.

These vulnerabilities are due to the incorrect handling of IGMP packets. An unauthenticated remote attacker would exploit these vulnerabilities by sending specifically crafted IGMP packets towards affected Cisco devices using Cisco IOS XR Software
.
On successful exploitation of these vulnerabilities would allow unauthenticated remote attacker to either immediately crash the Internet Group Management Protocol (IGMP) process, or cause memory exhaustion which eventually results in crash.

AFFECTED PRODUCTS

These vulnerabilities affect any Cisco device that is running any release of Cisco IOS XR Software, and its active interface is configured under multicast routing and it is receiving DVMRP traffic.

AFFECTED PRODUCTS

Determine Whether Multicast Routing Is Enabled:

• An administrator can determine whether multicast routing is enabled on a device by issuing the show igmp interface command.
• If the output of show igmp interface is empty, multicast routing is not enabled, and the device is not affected by these vulnerabilities.

Determine Whether the Device Is Receiving DVMRP Traffic:

• An administrator can determine whether the device is receiving DVMRP traffic by issuing the show igmp traffic command.
• If the DVMRP packets entry contains values of zero in the first column, and the counters remain zero on subsequent execution of the command, the device is not receiving DVMRP traffic.

These vulnerabilities result in memory exhaustion, and it is possible to recover the memory consumed by the IGMP process by restarting the IGMP process with the process restart igmp command

READ

- Cisco IOS XR Software DVMRP Memory Exhaustion Vulnerabilities

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

TA505 Threat Actors were found cybersquatting domains of popular brands including PayPal, Google, Microsoft, etc. for committing financial and consumer frauds

Severity: High

Date: September 02, 2020

IP ADDRESSES

217.182.227.117

Domain

amazon-india.online
apple.com.recover.support
com-finder-me.info
com-secure-login.info
facebook.com-account-login-manage.
yourfiresale.com
icloud.com-iphone.support
microsoft-alert.club
microsoft-sback-server.com
microsoft-store-drm-server.com
microsoft.com
xn--microsof-wyb.com
netflix-payments.com
netflixbrazilcovid.com
rbyroyalbank.com
safety.microsoft.com.mdmfmztwjj.l6ka
n7uf04p102xmpq.bid
samsungeblyaiphone.com
samsungpr0mo.online
secure-wellsfargo.org
store-in-box.com
stt-box.com
icloud.com-secure-login.info
4ever21.com
facebookwinners2020.com
micposoft.com
walrmart44.com
whatsalpp.com

JA3 PAIR

CLIENT:
6312930a139fa3ed22b87abb75c16afa
SERVER:
4192c0a946c5bd9b544b4656d9f624a
4

REMEDIATION

1. Immediately apply Security Patches for Microsoft vulnerabilities CVE-2020-1380, CVE-2020-1464, CVE-2020-1472, CVE-2020-1519, CVE-2020-1538, CVE-2020-1579, CVE-2020-1337, CVE-2020-0986, CVE-2020-0674, CVE- 2019-1429, CVE-2019-0676, & CVE-2018-8653 on Microsoft Windows Workstation and Server.
2. Ensure Microsoft Windows Servers are patched with latest security updates.
3. Ensure access controls are properly implemented and periodically evaluated for ATM Switch and SWIFT Network.
4. Ensure to closely monitor for any intrusion or suspicious activity on ATM Switch and SWIFT Network.
5. Ensure proper access controls are in place for NetBanking and Third-Party Payment Services.
6. Ensure to closely monitor for any intrusion or suspicious activity on NetBanking and Third-Party Payment services.
7. Ensure Domain Accounts follows least privilege principle and ensure TwoFactor authentication is enabled on all Business Email Accounts.
8. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel.
9. Ensure VPN client software and VPN servers are patched with latest security updates released by vendor.
10. Strictly ensure TCP Port 135, TCP Port 445, and TCP Port 3389 are not left open on Internet or DMZ facing side.
11. Please ensure TCP Port 135 (Remote Procedure Call - RPC), TCP Port 445 (Server Message Block - SMB), and TCP Port 3389 (Remote Desktop Protocol - RDP) are only accessible through VPN tunnel between VPN clients and Organization's Resources.
12. Ensure proper network segmentation are done, and ensure communication through TCP Port 135, TCP Port 445, and TCP Port 3389 are explicitly allowed on-demand only for particular network segments when needed.
13. Ensure network segments that allows communication over TCP Port 135, TCP Port 445, 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 3389, and unusual amount of data transmission, etc.
14. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
15. Ensure to monitor for excessive LDAP queries within 5 minutes from particular system, via SIEM solution.
16. Ensure VNC, SOCKS, and SMTP ports are also closely monitored.
17. 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.
18. Kindly Block IPs and Domains on the perimeter security devices.
19. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

READ

- Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

TA505 Threat Actors were found cybersquatting domains of popular brands including PayPal, Google, Microsoft, etc. for committing financial and consumer frauds

Severity: High

Date: September 02, 2020

HASHES (MD5)

HASHES	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
5acd6d9ac235104f90f9a39c11807c37cdfb1 03d6c151cc1a2e4e38bf3dbe41f	Yes	Yes	Yes	Yes	Yes
5acd6d9ac235104f90f9a39c11807c37cdfb1 03d6c151cc1a2e4e38bf3dbe41f	Yes	Yes	Yes	Yes	Yes
5acd6d9ac235104f90f9a39c11807c37cdfb1 03d6c151cc1a2e4e38bf3dbe41f	Yes	No	No	No	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

21st August 2020 – 27th August 2020 | TRAC-ID:NII20.08.0.4

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
August 27, 2020	Ubuntu Linux	USN-4477-1: Squid vulnerabilities	▪ Ubuntu 20.04 LTS	Security Patch Update
August 27, 2020	Ubuntu Linux	USN-4476-1: NSS vulnerability	▪ Ubuntu 20.04 LTS ▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS ▪ Ubuntu 14.04 ESM ▪ Ubuntu 12.04 ESM	Security Patch Update
August 27, 2020	Ubuntu Linux	USN-4475-1: Chrony vulnerability	▪ Ubuntu 20.04 LTS ▪ Ubuntu 18.04 LTS	Security Patch Update

REDHAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
August 26, 2020	Red Hat Enterprise Linux	RHSA-2020:3560	▪ Red Hat Enterprise Linux Server 6 x86_64 ▪ Red Hat Enterprise Linux Server 6 i386 ▪ Red Hat Enterprise Linux Workstation 6 x86_64 ▪ Red Hat Enterprise Linux Workstation 6 i386 ▪ Red Hat Enterprise Linux Desktop 6 x86_64 ▪ Red Hat Enterprise Linux Desktop 6 i386	Security Patch Update
August 26, 2020	Red Hat Enterprise Linux	RHSA-2020:3559	▪ Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.1 x86_64 ▪ Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.1 aarch64	Security Patch Update

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

21st August 2020 – 27th August 2020 | TRAC-ID: NII20.08.0.4

August 25, 2020	**Red Hat Enterprise Linux**	**RHSA-2020:3548**	▪ Red Hat Enterprise Linux Server 6 x86_64 ▪ Red Hat Enterprise Linux Server 6 i386 ▪ Red Hat Enterprise Linux Workstation 6 x86_64 ▪ Red Hat Enterprise Linux Workstation 6 i386 ▪ Red Hat Enterprise Linux Desktop 6 x86_64 ▪ Red Hat Enterprise Linux Desktop 6 i386	**Security Patch Update**
August 25, 2020	**Red Hat Enterprise Linux**	**RHSA-2020:3545**	▪ Red Hat Enterprise Linux for ARM 64 7 aarch64	**Security Patch Update**

IBM

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
August 27, 2020	**IBM Security Guardium**	**Multiple vulnerabilities in IBM Java SDK affect IBM Security Guardium**	▪ IBM Security Guardium 10.0 – 10.6 ▪ IBM Security Guardium 11.0 ▪ IBM Security Guardium 9.0 – 9.6	**Kindly update to fixed version**
August 26, 2020	**IBM Security Guardium Insights**	**IBM Security Guardium Insights is affected by IBM SDK, Java Technology Edition Quarterly CPU – Apr 2020 vulnerabilities**	▪ IBM Security Guardium Insights 2.0.1	**Kindly update to fixed version**