NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

October 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
Oracle Corporation released Critical Patch Updates (CPU) on October 2020, for Oracle products such as Oracle WebLogic, Oracle Database, Oracle Solaris, Oracle MySQL, Oracle VirtualBox, and Oracle JAVA	Critical
Remote Code Execution Vulnerability (CVE-2020-16898) in Microsoft Windows TCP/IP Stack that were widely exploited in targeted Malware Attack and Hacking Campaign	Critical
Microsoft Patch Tuesday – October 2020	Critical
Threat Actors that were found targeting Banking & Financial Institutions, and Retailers via POS Malware such as RtPOS, MMon (aka Kaptoxa), and PwnPOS	High
PoetRAT Malware that was found targeting State Government, Foreign Affairs, Critical Sectors, and Managed IT Service Providers	High
Kraken, a fileless Malware that was found abusing Windows Error Reporting service through APC Code Injection Technique	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

Oracle Corporation released Critical Patch Updates (CPU) on October 2020, for Oracle products such as Oracle WebLogic, Oracle Database, Oracle Solaris, Oracle MySQL, Oracle VirtualBox, and Oracle JAVA

Severity: Critical

Date: October 21, 2020

IMPACT

On successful exploitation of these vulnerabilities would allow remote attacker to gain unauthorized access, exfiltrate data, and cause disruption in business operations

REMEDIATION

1. Immediately apply available security patches for Oracle WebLogic, Oracle Database, Oracle Solaris, Oracle MySQL, Oracle VirtualBox, and Oracle JAVA SE.

2. Please refer attached Excel sheet for more details on exploitable CVE IDs, patch priority, and quick access to the security patches for respective Oracle products.

INTRODUCTION

Oracle Corporation released Critical Patch Updates (CPU) on October 2020, for Oracle products such as WebLogic, Oracle Database, Oracle Solaris, Oracle MySQL, Oracle VM VirtualBox, Oracle JAVA SE, and many other Oracle products.

Easily exploitable vulnerabilities in Oracle WebLogic Server (CVE-2020-14882, CVE-2020-14841, CVE-2020-14825, CVE-2020-14859, CVE-2020-14820, CVE-2020-14883), Oracle Database Server (CVE-2020-11023, CVE-2020-11023), Oracle Solaris (CVE-2020-14871), Oracle MySQL Server (CVE-2020-8174, CVE-2020-14828, CVE-2020-14827), and Oracle Java SE (CVE-2020-14803), would allow remote unauthenticated attacker with network access might compromise Oracle products.

On successful exploitation of these vulnerabilities would allow remote attacker to take complete control over Oracle products, gain unauthorized access to sensitive data, and execute ransomware like disruptive attack on enterprise wide network.
incident.

AFFECTED PRODUCTS

- Oracle WebLogic Server 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0,12.2.1.4.0, 14.1.1.0.0
- Oracle Database Server 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c
- Oracle Solaris 10, 11
- Oracle MySQL Server 5.6.49 and prior, 5.7.31 and prior, 7.3.30 and
- prior, 7.4.29 and prior, 7.5.19 and prior, 7.6.15 and prior, 8.0.21 and
- prior
- Oracle VM VirtualBox Prior to 6.1.16
- Oracle Java SE: 7u271, 8u261, 11.0.8, 15
- Oracle Java SE Embedded: 8u261

READ

- Oracle Critical Patch Update Advisory - October 2020
- October 2020 Critical Patch Update Released

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Remote Code Execution Vulnerability (CVE-2020-16898) in Microsoft Windows TCP/IP Stack that were widely exploited in targeted Malware Attack and Hacking Campaign

Severity: Critical

Date: October 15, 2020

IMPACT

On successful exploitation of this vulnerability would allow remote attacker to gain the ability to execute malicious code onto the target Windows server or client.

REMEDIATION

1. Ensure to apply security patches for this vulnerability (CVE-2020-16898), on Microsoft Windows Server and Workstation.

(Important Note:- Please refer attached Excel Sheet for quick access to the Security Patches. Just incase, if immediate patching for this vulnerability is not possible, then kindly apply the Temporary Mitigation)

TEMPORARY MITIGATION

1. Use the following PowerShell command to disable ICMPv6 RDNSS, to prevent attackers from exploiting this vulnerability. This solution is only applicable to Windows 1709 and higher:

PS C:\> netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=disable

(Note:- There is no need to restart Windows OS after making this changes.)

2. The above solution can be disabled using the following PowerShell command:

PS C:\> netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=enable

INTRODUCTION

Remote Code Execution Vulnerability (CVE-2020-16898) in Microsoft Windows TCP/IP Stack is widely exploited in targeted Malware Attack and Hacking Campaign.

This Remote Code Execution vulnerability exists within the Microsoft Windows TCP/IP stack that improperly handles ICMPv6 Router Advertisement packets, which allows remote attacker to send specifically crafted ICMPv6 Router Advertisement packets towards vulnerable Windows servers in remote location. On successful exploitation of this vulnerability would allow remote attacker to gain the ability to execute malicious code onto the target Windows server or client.

This Remote Code Execution vulnerability poses a severe risk of unauthorized access, data breach, disruptive malware like Ransomware attack to cause interruption in business operation, financial loss due to business downtime, and impact reputation of the organization post cyber incident.

AFFECTED PRODUCTS

- Windows Server version 2004/1909/1903 (Server Core installation)
- Windows Server 2019 and Windows Server 2019 (Server Core
- installation)
- Windows 10 Version 2004/1909/1903/1809/1803/1709 for x64-based
- Systems
- Windows 10 Version 2004/1909/1903/1809/1803/1709 for ARM64-
- based Systems
- Windows 10 Version 2004/1909/1903/1809/1803/1709 for 32-bit
- Systems

READ

- CVE-2020-16898 | Windows TCP/IP Remote Code Execution Vulnerability
- Threat Brief: Microsoft Vulnerability CVE-2020-16898
- Microsoft Windows TCP/IP Remote Code Execution Vulnerability (CVE-2020-16898)

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Microsoft Patch Tuesday – October 2020

Severity: Critical

Date: October 14, 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 87 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-2020-16905, CVE-2020-16909, CVE-2020-16896, CVE-2020-16897, CVE-2020-16939, CVE-2020-16907, and CVE-2020-16913) 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

- October 2020 Security Updates
- Microsoft October 2020 Patch Tuesday fixes 87 security bugs

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Threat Actors that were found targeting Banking & Financial Institutions, and Retailers via POS Malware such as RtPOS, MMon (aka Kaptoxa), and PwnPOS

Severity: High

Date: October 09, 2020

IP ADDRESSES

146.0.77.88
163.172.197.16
163.172.197.21

DOMAINS

writicipal.com
tkwait.writicipal.com

REMEDIATION

1. Ensure Microsoft Windows Servers are patched with latest security updates.
2. Ensure security measures for UPnP and SSDP services are in place and ensure these services (listening on multicast IP address 239.255.255.250) are isolated from untrusted networks, DMZ or Internet.
3. 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.
4. 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.
5. Ensure Domain Accounts follows least privilege principle and ensure TwoFactor 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, and TCP Port 3389 are not left open on Internet or DMZ facing side.
9. 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.
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

- VISA Warns of POS Malware Campaigns in North America

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Threat Actors that were found targeting Banking & Financial Institutions, and Retailers via POS Malware such as RtPOS, MMon (aka Kaptoxa), and PwnPOS

Severity: High

Date: October 09, 2020

HASHES (SHA-256)

Hashes	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
15712752daf007ea0db799a318412478c5a3a315a22932655c38ac6485f8ed00	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
e48af0380d51eff554d56aabeeb5087bba37fa8fb02af1ccd155bb8b5079edae	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
bdd978a91dad7a201274956098d0e6612e3f9e6a009fc4f24a362c19b1813218	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
5bc41cde297936199bd145098727905b75762dd85ff2e4caddb93e2370ff8fbc	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
cb7b7c6e37c4edd8bf9c2baaf3d97c895b705565aac7110ba3e7799d9e501172	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
e2f9cb1fcdc531583c82f40c7325118bbc671f4d33ea639f2d575fec96dbbd86	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
59adc06ae5a9504313229f252322d8a8e7826999ba1deb036172afd22c0a7774	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
663c69d8bb372487ca9bd8f3b6c983bf7388e79d2ecdb1713718a779f74b11d5	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
fb749c32b58fd1238f21d48ba1deb60e6fb4546f3a74e211f80a3ed005f9e046	YES	YES	YES	YES	YES
86dd21b8388f23371d680e2632d0855b442f0fa7e93cd009d6e762715ba2d054	YES	YES	YES	YES	YES
088f40a7a52635ff19e80c62883977d94dd5835e85739e19504f7437d296760b	YES	YES	YES	YES	YES
49c95e871d7e7f1286f592fe8d0a30b131fa9daa58824c8a6bdb78faf0b1f577	YES	YES	YES	YES	YES
d1fbb201844e0e012e63db65b177df6156cf930f4b5b7577a3f3e8c8a3f460ea	YES	YES	YES	YES	YES
4c7d57821c0642ceab5342b52328d4f2dbea59782d33ab08749e2ad6ba12ac3a	YES	YES	YES	YES	NO
6cf5e60480b505be5b8ddcd60d4a443cede840afe0bb29d09b885612bc04744a	NO	YES	YES	YES	NO
74da42b332e0254f2249b16d3643f84e8a5d466c5200fca81f9f728843df0ef6	YES	YES	YES	YES	YES
e691c0b3688e0664bbf2de18c560fd3dc516e789cec24421d345f0b709062b3c	NO	YES	YES	YES	NO
93f2b6436d74bc009542e0b0b643f034803d21e7a9c24e20c14adc121f60a3c1	YES	YES	YES	NO	YES
1f1ada65aac84d54c066f90d9cada551829e2bd1e9399c8d9f7cbbcdbded68cd	YES	YES	YES	NO	YES
a5bc7c865c170b0fdb383e5a007c76de5c06013dc3f394e41a8b58a0f0b5cf35	YES	YES	YES	YES	NO

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

PoetRAT Malware that was found targeting State Government, Foreign Affairs, Critical Sectors, and Managed IT Service Providers

Severity: High

Date: October 09, 2020

IP ADDRESSES

47.240.73.77
114.67.110.37
124.232.170.16
47.246.22.228
47.246.17.230

DOMAINS

slimip.accesscam.org
dellgenius.hopto.org
insiderppe.cloudapp.net
dbs24support.com
ueteioniansd.hopto.org
ksb-arching.hopto.org
htelementb.hopto.org
utmachinetool.hopto.org
ueteionians.hopto.org
gbfairunqh.hopto.org
ieickelmgq.hopto.org
halamusfilbas.hopto.org
aoolhousag.hopto.org
ns1.support-team.live
dellgenius.hopto.org
mail.thefastway.biz
thefastway.biz

REMEDIATION

1. Immediately apply Security Patches for Microsoft vulnerabilities CVE-2020-1472, CVE-2020-1396, CVE-2020-1429, & CVE-2020-1197 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

- PoetRAT: Malware targeting public and private sector in Azerbaijan evolves

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

PoetRAT Malware that was found targeting State Government, Foreign Affairs, Critical Sectors, and Managed IT Service Providers

Severity: High

Date: October 09, 2020

HASHES (SHA-256)

Hashes	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
dc565146cd4ecfb45873e44aa1ea1bac8cfa8fb086140154b429ba7274cda9a2	YES	YES	YES	YES	YES
64aeffe15aece5ae22e99d9fd55657788e71c1c52ceb08e3b16b8475b8655059	YES	YES	NO	YES	YES
ac4e621cc5895f63a226f8ef183fe69e1ae631e12a5dbef97dd16a6dfafd1bfc	YES	YES	YES	YES	YES
a703dc8819dca1bc5774de3b6151c355606e7fe93c760b56bc09bcb6f928ba2d	YES	YES	YES	YES	YES
208ec23c233580dbfc53aad5655845f7152ada56dd6a5c780d54e84a9d227407	YES	YES	YES	YES	YES
e4e99dc07fae55f2fa8884c586f8006774fe0f16232bd4e13660a8610b1850a2	YES	YES	YES	NO	YES
d4b7e4870795e6f593c9b3143e2ba083cf12ac0c79d2dd64b869278b0247c247	YES	NO	YES	YES	YES
d5d7fad5b745fa04f7f42f61a1db376f9587426c88ce276f06de8ea6889dfae8	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
31c327a3be44e427ae062c600a3f64dd9125f67d997715b63df8d6effd609eb3	NOT KNOWN	YES	YES	YES	YES
b1e7dc16e24ebeb60bc6753c54e940c3e7664e9fcb130bd663129ecdb5818fcd	NO	NO	YES	YES	YES
4eb83253e8e50cd38e586af4c7f7db3c4aaddf78fb7b4c563a32b1ad4b5c677c	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
746fbdee1867b5531f2367035780bd615796ebbe4c9043134918d8f9240f98b9	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
f842354198cfc0a3296f8d3c6b38389761674f1636129836954f50c2a7aab740	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
312f54943ebfd68e927e9aa95a98ca6f2d3572bf99da6b448c5144864824c04d	YES	NO	YES	YES	YES
252c5d491747a42175c7c57ccc5965e3a7b83eb5f964776ef108539b0a29b2ee	YES	NO	YES	YES	YES
37118c097b7dbc64fa6ac5c7b28ebac542a72e926d83564732f04aaa7a93c5e3	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
d605a01e42d5bb6bca781b7ba32618e2f2870a4624b50d6e3d895e8e96adee6a	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
970793967ecbe58d8a6b54f5ec5fd2551ce922cb6b3584f501063e5f45bdd58a	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN	NOT KNOWN
a3405cc1fcc6b6b96a1d6604f587aee6aafe54f8beba5dcbaa7322ac8589ffde	YES	YES	YES	YES	YES
ca8492139c556eac6710fe73ba31b53302505a8cc57338e4d2146bdfa8f69bdb	NO	NO	YES	YES	YES

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Kraken, a fileless Malware that was found abusing Windows Error Reporting service through APC Code Injection Technique

Severity: High

Date: October 08, 2020

IP ADDRESSES

51.158.113.130

DOMAIN

yourrighttocompensation.com
asia-kotoba.net

URL

https<://>yourrighttocompensation.com/ping
https<://>yourrighttocompensation.com/?rid=UNfxeHM
https<://>yourrighttocompensation.com/download/?key=15a50bfe99cfe29da475bac45fd16c50c60c85bff6b06e530cc91db5c710ac30&id=0
https<://>yourrighttocompensation.com/?rid=n6XThxD
https<://>yourrighttocompensation.com/?rid=AuClILU
https<://>asia-kotoba.net/favicon32.ico

REMEDIATION

1. Immediately apply Security Patches for Microsoft vulnerabilities CVE-2020-1396, CVE-2020-1429, & CVE-2020-1197 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, URLs, 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

- Release the Kraken: Fileless APT attack abuses Windows Error Reporting service

HASH (SHA-256)

Hashes	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
31368f805417eb7c7c905d0ed729eb1bb0fea33f6e358f7a11988a0d2366e942	Yes	Yes	Yes	Yes	Yes
d68f21564567926288b49812f1a89b8cd9ed0a3dbf9f670dbe65713d890ad1f4	Yes	Yes	Yes	Yes	Yes
e36d6c2da2438e390e4564bf5682248e2d5622af10a6b1763668a45a965f24d7	No	No	No	No	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

16th October 2020 – 22nd October 2020 | TRAC-ID: NII20.10.0.3

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
October 22, 2020	Ubuntu Linux	USN-4601-1: pip vulnerability	▪ Ubuntu 18.04 LTS	Security Patch Update
October 22, 2020	Ubuntu Linux	USN-4600-1: Netty vulnerabilities	▪ Ubuntu 16.04 LTS	Security Patch Update
October 22, 2020	Ubuntu Linux	USN-4593-2: FreeType vulnerability	▪ Ubuntu 14.04 ESM	Security Patch Update

REDHAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
October 22, 2020	Red Hat Enterprise Linux	RHSA-2020:4307	▪ 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
October 22, 2020	Red Hat Enterprise Linux	RHSA-2020:4306	▪ 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

16th October 2020 – 22nd October 2020 | TRAC-ID: NII10.03.0.3

October 22, 2020	**Red Hat Enterprise Linux**	**RHSA-2020:4305**	▪ Red Hat Enterprise Linux for x86_64 8 x86_64 ▪ Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.2 x86_64 ▪ Red Hat Enterprise Linux Server - AUS 8.2 x86_64 ▪ Red Hat Enterprise Linux Server - TUS 8.2 x86_64 ▪ Red Hat Enterprise Linux for ARM 64 8 aarch64 ▪ Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.2 aarch64	**Security Patch Update**

IBM

October 20, 2020	**IBM i**	**BIND for IBM i is affected by CVE-2020-8622 and CVE-2020-8624**	▪ IBM i 7.4 ▪ IBM i 7.3 ▪ IBM i 7.2 ▪ IBM i 7.1	**Kindly update to fixed version**
October 20, 2020	**IBM QM**	**IBM MQ could allow leak sensitive information due to an error within the pre-v7 pubsub logic (CVE-2020-4319)**	▪ IBM MQ 9.1 LTS ▪ IBM MQ 9.0 LTS ▪ IBM MQ 8.0 ▪ IBM MQ 9.1 CD ▪ IBM WebSphere MQ 7.5 ▪ IBM WebSphere MQ 7.1	**Kindly update to fixed version**