NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

November 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
A Microsoft Patch Tuesday – November 2020	Critical
xHunt Hacking Campaigns which were found targeting Government, Shipping and Transportation organizations in the Middle East and other part of the world	Critical
A Threat Actor Group "UNC1945" which was found to be targeting Banking & Financial Institutions, and Managed Service Providers using Malware and Exploitation Techniques	Critical
Remote Code Execution (CVE-2020-14882) and Elevation of Privilege (CVE-2020-14883) vulnerabilities within Console component of Oracle WebLogic Server, which were widely exploited in targeted Malware Attacks and Hacking Campaigns	Critical

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

A Microsoft Patch Tuesday – November 2020

Severity: Critical

Date: November 12, 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 112 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 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 Internet Explorer, Defender, and Office products

READ

- November 2020 Security Updates
- Microsoft November 2020 Patch Tuesday fixes 112 vulnerabilities

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

xHunt Hacking Campaigns which were found targeting Government, Shipping and Transportation organizations in the Middle East and other parts of the world

Severity: Critical

Date: November 11, 2020

DOMAIN

deman1.icu
hotsoft.icu
uplearn.top
lidarcc.icu
sharepoint-web.com

REMEDIATION

1. Ensure to apply latest Security Patches for Microsoft Windows Server, Microsoft Exchange Server, Microsoft SharePoint Server, and IIS Server.
2. Ensure to apply latest security patches on Cisco ASA Firewall, nd F5 BIG-IP Load Balancer.
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 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, 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 Port 1900, and TCP Port 3389, 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

- xHunt Campaign: Newly Discovered Backdoors Using Deleted Email Drafts and DNS Tunneling for Command and Control

HASH (SHA-256)

Hashes	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
407e5fe4f6977dd27bc0050b2ee8f04b398e9bd28edd9d4604b782a945f8120f	Not Known	Not Known	Not Known	Not Known	Not Known
c18985a949cada3b41919c2da274e0ffa6e2c8c9fb45bade55c1e3b6ee9e1393	Not Known	Not Known	Not Known	Not Known	Not Known
6c13084f213416089beec7d49f0ef40fea3d28207047385dda4599517b56e127	No	Yes	No	No	No
efaa5a87afbb18fc63dbf4527ca34b6d376f14414aa1e7eb962485c45bf38372	No	Yes	No	No	No

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A Threat Actor Group "UNC1945" which was found to be targeting Banking & Financial Institutions, and Managed Service Providers using Malware and Exploitation Techniques

Severity: Critical

Date: November 11, 2020

IP SUBNETS

46.30.189.0/24
66.172.12.0/24

REMEDIATION

1. Immediately apply Security Patches for Oracle Solaris OS vulnerability CVE-2020-14871.
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 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.
4. Ensure Domain Accounts follows least privilege principle and ensure TwoFactor 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 Port 1900, 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).
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 IP Subnets on the perimeter security devices.
14. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

READ

- UNC1945, a sophisticated threat actor used Oracle Solaris Zero-Day exploit
- Live off the Land? How About Bringing Your Own Island? An Overview of UNC1945
- In Wild Critical Buffer Overflow Vulnerability in Solaris Can Allow Remote Takeover — CVE-2020-14871
- CVE-2020-14871 | NIST Detail on vulnerability in the Oracle Solaris product of Oracle Systems

HASH (SHA-256)

Hashes	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
c94fdfedd40e0b194165294f48497794 7df9da2000cb8fe02243961384b249ff	No	No	No	No	No
7d587a5f6f36a74dcfbcbaecb2b0547fdf 1ecdb034341f4cc7ae489f5b57a11d	No	Yes	No	No	No
3c2fe308c0a563e06263bbacf793bbe9b 2259d795fcc36b953793a7e499e7f71	Yes	Yes	yes	yes	Yes
14296b21c6e2ba9d56759e2da4b09f58 148852ddeefa8fb76a838a30871679a7	No	No	No	No	No

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Remote Code Execution (CVE-2020-14882) and Elevation of Privilege (CVE-2020-14883) vulnerabilities within Console component of Oracle WebLogic Server, which were widely exploited in targeted Malware Attacks and Hacking Campaigns

Severity: Critical

Date: October 30, 2020

IMPACT

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.

REMEDIATION

1. Immediately update or upgrade Oracle WebLogic server to latest version, higher than affected versions.

2. Kindly block IP Addresses, URLs, and Hashes on respective security devices. (refer Excel sheet)

3. 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

Remote Code Execution (CVE-2020-14882) and Elevation of Privilege (CVE-2020-14883) vulnerabilities within Console component of Oracle WebLogic Server, is widely exploited in targeted Malware Attack and Hacking Campaign.

Easily exploitable Remote Code Execution vulnerability (CVE-2020-14882) allows unauthenticated remote attacker with network access via HTTP, to send specifically crafted malicious requests and compromise affected Oracle WebLogic Server.

Easily exploitable Elevation of Privilege vulnerability (CVE-2020-14883) allows authenticated remote attacker with network access via HTTP, to elevate permissions for gaining administrative access and compromise affected Oracle WebLogic Server.

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.

access to sensitive data, and execute ransomware like disruptive attack on enterprise wide network.
incident.

AFFECTED PRODUCTS

- Oracle WebLogic Server versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, and 14.1.1.0.0.

READ

- Oracle Critical Patch Update Advisory - October 2020
- CVE-2020-14882 Detail | NIST
- CVE-2020-14883 Detail | NIST
- Critical Oracle WebLogic flaw actively targeted in attacks

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

23rd October 2020 – 1st November 2020 | TRAC-ID: NII20.11.0.1

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
October 28, 2020	Ubuntu Linux	USN-4610-1: fastd vulnerability	▪ Ubuntu 20.04 LTS	Security Patch Update
October 28, 2020	Ubuntu Linux	USN-4609-1: GOsa vulnerabilities	▪ Ubuntu 16.04 LTS	Security Patch Update
October 28, 2020	Ubuntu Linux	USN-4552-3: Pam-python regression	▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS	Security Patch Update

REDHAT

October 28, 2020	Red Hat JBoss Enterprise Application	RHSA-2020:4402	▪ JBoss Enterprise Application Platform Text-Only Advisories x86_64	Security Patch Update
October 28, 2020	Red Hat JBoss Enterprise Application	RHSA-2020:4401	▪ JBoss Enterprise Application Platform 7.3 for RHEL 8 x86_64 ▪ JBoss Enterprise Application Platform 7.3 for RHEL 7 x86_64 ▪ JBoss Enterprise Application Platform 7.3 for RHEL 6	Security Patch Update

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

23rd October 2020 – 1st November 2020 | TRAC-ID: NII10.11.0.1

October 28, 2020	**Red Hat JBoss Core Services**	RHSA-2020:4384	▪ Red Hat JBoss Core Services 1 for RHEL 7 x86_64 ▪ Red Hat JBoss Core Services 1 for RHEL 6 x86_64 ▪ Red Hat JBoss Core Services 1 for RHEL 6 i386	Security Patch Update
October 28, 2020	**Red Hat JBoss Core Services**	RHSA-2020:4383	▪ Red Hat JBoss Core Services Text-Only Advisories x86_64	Security Patch Update

IBM

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
October 28, 2020	**IBM QRadar Wincollect**	IBM QRadar Wincollect is vulnerable to improper access control (CVE-2020-4485, CVE-2020-4486)	▪ IBM QRadar Wincollect 7.2.0 – 7.2.9	Kindly update to fixed version
October 27, 2020	**IBM WebSphere Application Server**	WebSphere Application Server Admin Console is vulnerable to a directory traversal vulnerability (CVE-2020-4782)	▪ IBM WebSphere Application Server 9.0 ▪ IBM WebSphere Application Server 8.5 ▪ IBM WebSphere Application Server 8.0 ▪ IBM WebSphere Application Server 7.0	Kindly update to fixed version