NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

April 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
Microsoft SMBv3 vulnerability (CVE-2020-0796) in Microsoft Windows Products, found widely exploited in Malware and Hacking Campaigns.	Critical
A Remote Code Execution vulnerability (CVE-2020-10189) in Zoho's ManageEngine Desktop Central, found widely exploited by APT41 Chinese Threat Actors.	Critical
Attackers are leveraging and targeting Zoom platform for hijacking teleconferencing, and compromise Windows computers during COVID-19 pandemic.	Critical
New Nefilim Ransomware found targeting Managed IT Service providers of Critical Sectors such as Oil & Gas Industries, Power Grid, and Raw Material Producers	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

Microsoft SMBv3 vulnerability (CVE-2020-0796) in Microsoft Windows Products, found widely exploited in Malware and Hacking Campaigns

Severity: Critical

Date: April 03, 2020

IMPACT

On successful exploitation of this vulnerability would allow remote attacker to gain unauthorized access and execute malicious code in context of user account and take ownership of the affected Microsoft Products.

EXPLOITABLE CVE IDs

- CVE-2020-0796

REMEDIATION

1. Kindly apply available patches for Microsoft SMBv3 vulnerability on Microsoft Windows Workstations & Servers.

2. Kindly refer attached Excel Sheet, for quick access to the Security Patches.

INTRODUCTION

A Remote Code Execution vulnerability (CVE-2020-0796) within Microsoft Server Message Block (SMBv3) protocol in Microsoft Windows products, found widely exploited in Malware Attacks and Hacking Campaigns

.

The vulnerability exists in the way Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests. On successful exploitation of this vulnerability would allow attackers to gain unauthorized access and gives them an ability to execute malicious code on to the target server or workstation.

IMPORTANT

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 10 Version 1903 for 32-bit Systems
- Microsoft Windows 10 Version 1903 for x64-based Systems
- Microsoft Windows 10 Version 1903 for ARM64-based Systems
- Microsoft Windows Server, version 1903 (Server Core installation)
- Microsoft Windows 10 Version 1909 for 32-bit Systems
- Microsoft Windows 10 Version 1909 for x64-based Systems
- Microsoft Windows 10 Version 1909 for ARM64-based Systems
- Microsoft Windows Server, version 1909 (Server Core installation)

READ

- CVE-2020-0796 | Windows SMBv3 Client/Server Remote Code Execution Vulnerability

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A Remote Code Execution vulnerability (CVE-2020-10189) in Zoho's ManageEngine Desktop Central, found widely exploited by APT41 Chinese Threat Actors

Severity: Critical

Date: April 03, 2020

IMPACT

On successful exploitation of this vulnerability would allow unauthenticated remote attackers to execute arbitrary code on affected installations of Zoho's ManageEngine Desktop Central.

EXPLOITABLE CVE IDs

• CVE-2020-10189

REMEDIATION

1. Kindly upgrade ManageEngine Desktop Central to either fixed version 10.0.479 or latest version 10.0.482.

2. Strictly follow these steps for Identification and Mitigation of this vulnerability CVE-2020-10189.

3. Ensure to follow these Important instructions to Apply Services Packs & Hot Fixes

INTRODUCTION

A Remote Code Execution vulnerability (CVE-2020-10189) in Zoho's ManageEngine Desktop Central, found widely exploited by Chinese APT41 Threat Actors.

On successful exploitation of this vulnerability would allow unauthenticated remote attackers to execute arbitrary code on affected installations of Zoho's ManageEngine Desktop Central.

IMPORTANT

- The complete fix for this remote code execution vulnerability (CVE-2020-10189) is now available in build 10.0.479.
- This vulnerability will not impact Secure Gateway Server.Customers using builds that include the short-term fix are notvulnerable to exploitation attack.
- Complete details on Identification and Mitigation of this remote code execution vulnerability (CVE-2020-10189) in Zoho's ManageEngine Desktop Central, can be found here.
- Important instructions to Apply Service Packs & Hot Fixes, can befound here.

AFFECTED PRODUCTS

• ManageEngine Desktop Central version prior to 10.0.479

READ

- ManageEngine Desktop Central remote code execution vulnerability (CVE-2020-10189)
- Identification and mitigation of remote code execution vulnerability CVE-2020-10189
- Instructions to Apply Service Packs & Hot Fixes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Attackers are leveraging and targeting Zoom Video Communication platform for hijacking the teleconferencing or online classroom, and compromise Windows computers during COVID-19 pandemic

Severity: Critical

Date: April 06, 2020

IMPACT

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

REMEDIATION

1. Kindly update Zoom software to latest version 4.6.9 (19253.0401).

2. Kindly apply available patches for Microsoft SMBv3 vulnerability on Microsoft Windows Workstations & Servers.

3. Restrict sharing of Zoom Meeting Invitation links to only intended attendees or recipients.

4. Avoid using Personal Meeting ID (PMI) to host public events.

5. Ensure to use Waiting Room feature for hosts, to control who comes and goes.

6. Allow only host to share the screen during Zoom meeting.

7. Allow only signed-in users to join Zoom meeting.

8. Ensure Zoom meeting requires password prior to joining.

9. Ensure to turn off File Transfer, Private Chat, and Annotation.

10. Ensure to Enable or Disable video, and mute participants wherever needed.

INTRODUCTION

Attackers are leveraging and targeting Zoom Video Communication platform for hijacking the teleconferencing or online classroom, and compromise Windows computers during COVID-19 pandemic.

As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected in the wake of the COVID-19 crisis, incidents related to VTC hijacking (aka, Zoom-bombing) are emerging worldwide. Multiple incidents have been reported concerning to conferences being disrupted by pornographic and/or hate images and threatening language.

Attackers are taking advantage of publicly available Zoom Meeting Invitation Links and Zoom Meeting IDs, allowing them to randomly join the Meeting Room and causing interference or embarrassment situation during the video-teleconferencing (VTC).

Attackers are also taking advantage of a 'UNC path injection' vulnerability in Zoom video conferencing software (for Windows) as well as a Remote Code Execution vulnerability (CVE-2020-0796) within Microsoft Server Message Block (SMBv3) protocol, to steal Windows login credentials and execute arbitrary commands onto the affected Windows systems.

AFFECTED PRODUCTS

- Zoom version prior to 4.6.9 (19253.0401)
- Microsoft Windows 10 Version 1903 for 32-bit Systems
- Microsoft Windows 10 Version 1903 for x64-based Systems
- Microsoft Windows 10 Version 1903 for ARM64-based Systems
- Microsoft Windows Server, version 1903 (Server Core installation)
- Microsoft Windows 10 Version 1909 for 32-bit Systems
- Microsoft Windows 10 Version 1909 for x64-based Systems
- Microsoft Windows 10 Version 1909 for ARM64-based Systems
- Microsoft Windows Server, version 1909 (Server Core installation)

READ

- How to Keep Uninvited Guests Out of Your Zoom Event
- New Zoom Hack Lets Hackers Compromise Windows and Its Login Password
- FBI Warns of Teleconferencing Hijacking During COVID-19 Pandemic

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

New Nefilim Ransomware found targeting Managed IT Service providers of Critical Sectors such as Oil & Gas Industries, Power Grid, and Raw Material Producers

Severity: Critical

Date: April 07, 2020

IP ADDRESSES

203.208.51.148
203.208.43.228
203.208.43.216

EMAIL ADDRESSES

jamesgonzaleswork1972<@>protonmail.com
pretty_hardjob2881<@>mail.com
dprworkjessiaeye1955<@>tutanota.com
derekvirgil<@>protonmail.com
samanthareflock<@>mail.com
gerardbroncks<@>tutanota.com

REMEDIATION

1. Immediately apply Security Patches for Microsoft SMB & other critical vulnerabilities CVE-2020-0796, CVE-2020-0872, CVE-2020-0684, CVE-2020-0852, CVE-2020-0768, CVE-2020-0788, CVE-2020-0824, CVE-2020-0834, CVE-2020-0847, CVE-2020-0877, & CVE-2020-0887 on Windows Workstation and Server.
2. Immediately apply Security Patches for Microsoft vulnerabilities CVE-2020-0645,CVE-2020-0795, CVE-2020-0891, CVE-2020-0893, CVE-2020-0894, & CVE-2020-0903 on Microsoft IIS, SharePoint and Exchange Servers.
3. Strictly use least privilege accounts throughout the enterprise wide network.
4. Ensure to enable Two-Factor Authentication on business email accounts.
5. Ensure to Disable SMB version 1 (SMBv1) on Windows server.
6. Ensure TCP Port 3389 (RDP), TCP Port 135 (RPC), and TCP Port 445 (SMB) are only accessible through VPN tunnel between VPN clients and organization resources.
7. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to organization resources via VPN tunnel.
8. Ensure VPN client software and VPN servers are patched with latest security updates released by vendor.
9. Strictly ensure TCP Port 3389, TCP Port 135, & TCP Port 445 are not left open on Internet or DMZ facing side.
10. Ensure proper network segmentation are done and ensure communication through TCP Port 3389, TCP Port 135, & TCP Port 445 are explicitly allowed ondemand only for particular network segments when needed.
11. Ensure network segments that allows communication over TCP Port 3389, TCP Port 135, & TCP Port 445 are strictly monitored for any anomaly or suspicious patterns like lateral movement, excessive network traffics on TCP Port 3389, TCP Port 135, & TCP Port 445, unusual amount of data transmission, etc.
12. Kindly Block IPs and Emails on the perimeter security devices.
13. Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

READ

- Nefilim Ransomware Threatens to Expose Stolen Data
- New Nefilim Ransomware Threatens to Release Victims' Data

HASHES (SHA-256)

Hashes	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
5ab834f599c6ad35fcd0a168d93c52c399c6de7d1c20f33e25cb1fdb25aec9c6	YES	YES	YES	NO	YES
d4492a9eb36f87a9b3156b59052ebaf10e264d5d1ce4c015a6b0d205614e58e3	NOT KNOWN	YES	YES	NO	YES

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

30th March 2020 – 05th April 2020 | TRAC-ID: NII20.04.0.1

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
April 04, 2020	Ubuntu Linux	USN-4317-1: Firefox vulnerabilities	▪ Ubuntu 19.10 ▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS	Security Patch Update
April 02, 2020	Ubuntu Linux	USN-4316-2: GD Graphics Library vulnerabilities	▪ Ubuntu 14.04 ESM	Security Patch Update

REDHAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
April 01, 2020	Red Hat Enterprise Linux	RHSA-2020:1270	▪ 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

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

30th March 2020 – 05th April 2020 | TRAC-ID: NII20.04.0.1

March 31, 2020	**Red Hat Enterprise Linux**	RHSA-2020:1234	▪ Red Hat Enterprise Linux Server 7 x86_64	Security Patch Update
March 31, 2020	**Red Hat Enterprise Linux**	RHSA-2020:1231	▪ Red Hat Enterprise Linux Server 7 x86_64 ▪ Red Hat Enterprise Linux Workstation 7 x86_64	Security Patch Update

SUSE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
April 03, 2020	**SUSE Linux**	Security update for exiv2	▪ SUSE Linux Enterprise Module for Open Buildservice Development Tools 15-SP1 ▪ SUSE Linux Enterprise Module for Desktop Applications 15-SP1	Kindly update to fixed version
April 03, 2020	**SUSE Linux**	Security update for libxslt	▪ SUSE Linux Enterprise Server 12-SP5 ▪ SUSE Linux Enterprise Server 12-SP4	Kindly update to fixed version
April 03, 2020	**SUSE Linux**	Security update for bluez	▪ SUSE Linux Enterprise Workstation Extension 15-SP1 ▪ SUSE Linux Enterprise Module for Desktop Applications 15-SP1 ▪ SUSE Linux Enterprise Module for Basesystem 15-SP1	Kindly update to fixed version