NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

August 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

(CVE-2020-1380, CVE-2020-1464, CVE-2020-1472,CVE-2020-1519, CVE-2020-1538, CVE-2020-1579) in Microsoft Server products, widely exploited in targeted malware attacks and hacking campaigns.

Critical

The SANS Institute, a cybersecurity training organization suffered security breach followed by data breach incident.

High

Canon Inc., a Japanese-based optical products company suffered security breach followed by massive data breach incident caused by Maze Ransomware Operator.

High

Multiple vulnerabilities in Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS) can be taken advantage by attackers in hacking campaign.

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

(CVE-2020-1380, CVE-2020-1464, CVE-2020-1472, CVE-2020-1519, CVE-2020-1538, CVE-2020-1579) in Microsoft Server products, widely exploited in targeted malware attacks and hacking campaigns.

Severity: Critical

Date: August 13, 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 the 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 120 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 the user account.

And also, Microsoft released security patches for very critical vulnerabilities (CVE-2020-1380, CVE-2020-1464, CVE-2020-1472, CVE-2020-1519, CVE-2020-1538, CVE-2020-1579) in Microsoft Windows Workstation and Server products that are widely exploited in targeted malware attacks and hacking campaigns.

IMPORTANT

Microsoft Windows 10 1803 has reached the 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, .NET, and SharePoint Servers products.
- Microsoft Internet Explorer, and Office products.

READ

- August 2020 Security Updates
- Microsoft August 2020 Patch Tuesday fixes 2 zero-days, 120 flaws

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

The SANS Institute, a cybersecurity training organization, suffered a security breach followed by data breach incident.

Severity: High

Date: August 12, 2020

RECOMMENDATION

1. Strictly avoid downloading any attachment or clicking on website link received in Spam, Phishing, or any untrusted email from unknown sender.

2. Always stick to the Zero-Trust approach while dealing with day to day activities during business and non-business hours.

3. Always ensure to have Multi-Factor Authentication for your business email account, instead of solely relying on TwoFactor Authentication.

4. Ensure Configuration Review is timely conducted at least fortnightly or monthly, to detect any unauthorized changes and misconfiguration issues in Business Email Account or service. And, ensure to review installed Office365 Add-ons.

5. Immediately apply security patches for Microsoft vulnerability CVE-2020-1147 on Microsoft Windows Server, and Microsoft SharePoint Server.

6. Ensure to immediately patch UPnP related vulnerabilities CVE-2020-1354 and CVE-2020-1430, on Windows Server or Workstation.

7. Ensure security measures for UPnP (Universal Plug and Play) and SSDP (Simple Service Discovery Protocol) 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.

8. Ensure to closely monitor for any intrusion or suspicious activities on the system and network, via SIEM solution through managed SOC service

INCIDENT BRIEFING

The SANS Institute, a cybersecurity training organization, suffered a security breach followed by data breach incident.

On August 06, 2020, The SANS Institute got aware of the security breach during the review process of their organization's email configuration.

The internal investigation reveals that one of their employees fall victim to a phishing attack which allowed a remote attacker to gain unauthorized access to the victim's email account.

The internal investigation further reveals that since the phishing attack was specifically directed towards a particular employee, which as a result impacted a single employee's email account and no other accounts or systems were compromised

The internal investigation further reveals that remote attacker made unauthorized configuration changes by creating a rule which allowed them to forwarad , a total of 513 emails received on the victim's email account to attack's controlled email account and the forwarded emails contained approximately 28,000 records of personally identifiable information (PII) associated with SANS members such as email addresses, full names, phone numbers, work title, company names and physical addresses.

The remote attack further installed a malicious Office365 Add-on (more likely obfuscated Office365 Oauth app) to retain persistent access onto the victim's email account.

Considering the nature of this targeted phishing attack, which did not intended to steal login credential (username and password) of the victim's email account, but rather hijack the victim's email account through Microsoft OAuth API to retain persistent access onto the victim's email account and his data accessibleon Microsoft Office365 Email Account.

LESSON LEARNED

- Do not solely rely on Two-Factor Authentication, instead ensure to have Multi-Factor Authentication in place to prevent unauthorized access.
- Timely configuration review (at least fortnightly or monthly) can help detectany unauthorized changes and misconfiguration issues at very early stage,to contain damage caused by data breach or security breach incidents.
- Always stick to the Zero-Trust approach and stay vigilant while dealing with day to day activities during business and non-business hours

READ

- SANS infosec training org suffers data breach after phishing attack
- SANS Data Incident 2020

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Canon Inc., a Japanese-based optical products company suffered security breach followed by massive data breach incident caused by Maze Ransomware Operator

Severity: hIgh

Date: August 06, 2020

RECOMMENDATION

1. Ensure Amazon Web Service (Amazon EC2, Amazon ELB, Amazon CloudFront, Amazon RDS, and Amazon S3 Bucket) follows best security practices and access controls are timely reviewed.

2. Ensure Remote Desktop (RDP), Remote Procedure Call (RPC), and Virtual Network Computing (VNC) Services are strictly isolated from internet facing cloud or onpremise IT infrastructure. And ensure these remote services are only allowed through VPN tunnels.

3. Ensure vulnerable SMB protocols, are strictly disabled from internet facing cloud or on-premise IT infrastructure. And ensure SMB must be used in controlled environment, and only be used when filesharing is required.

4. Ensure Remote Desktop service is strictly prohibited on servers, that stores sensitive data.

5. Ensure network segmentation is done properly and ensure sensitive data hosting servers are completely isolated from other networks or systems.

6. Ensure to closely monitor for any intrusion or suspicious activities on the system and network, via SIEM solution throughmanaged SOC service.

7. Procure services to detect Personally Identifiable Information (PII) over the Internet and Darkweb related to your organization/brand.

8. Ensure to implement the process for ThirdParty vendors, to restrict sharing and retention of sensitive or PII data.

INCIDENT BRIEFING

Canon Inc., a Japanese-based optical products company suffered security breach followed by massive data breach incident caused by Maze Ransomware Operator.

On July 30, 2020, one of the Canon Inc.'s site "image.canon" suffered an unexpected outage that resulted in data loss, which involves Photo and Video Image files stored on the Amazon AWS cloud hosting server.

On August 04, 2020, Canon Inc. confirmed that some of the photo and video image files saved on their 10GB long-term storage prior to June 16, 2020 09:00AM (JST) are lost, but the still image thumbnails of the affected (or lost) files are not affected nor image data was leaked.

Later, on August 05, 2020, Canon Inc.'s IT department had sent a companywide notification stating that "Canon USA is experiencing widespread system issues, affecting multiple applications, Teams, Email, and other systems may not be available at this time."

The on-going investigation further reveals that this outage was caused by Maze Ransomware Operator, and Maze Ransomware Operator claimed to have exfiltrate 10TB of data prior to executing Maze Ransomware attack.

Canon Inc. continued to investigate this severe security breach incident, to collect further artifacts and determine scope of data & IT Infrastructure compromise

THREAT INTELLIGENCE ANALYSIS

Following the news, our Threat Intelligence Team at Network Intelligence (I) Pvt. Ltd. did their analysis on the security breach incident caused by Maze Ransomware Operator.

The analysis from our Threat Intelligence Team reveals that, the Canon Inc. was an easiest target considering the exposure of their on-premise IT infrastructure located in Melville city, New York, USA. The Maze Ransomware Operator gained unauthorized access onto the two servers located in Melville city, which was hosting 22 business services and multiple databases. The Maze Ransomware Operator took advantage of publicly exposed Remote Desktop (RDP), Remote Procedure Call (RPC), Virtual Network Computing (VNC), and Telnet services running on both the servers.

Our Threat Intelligence Team further added that, such loose security in either cloud or on-premise IT infrastructure often gives easy access to cyber criminals in few attempts within a day or two. Timely review of cloud security measures including misconfiguration issues, is what we strongly recommend to our customers from cross organizational sectors.

READ

- Canon hit by Maze Ransomware attack, 10TB data allegedly stolen

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Multiple vulnerabilities in Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS) can be taken advantage by attackers in hacking campaign

Severity: Critical

Date: July 29, 2020

IMPACT

The business impact that these vulnerabilities might cause are, unauthorized access, data breach, security breach, breach of customer trust, disruption in business operations, and may impact reputation of an organization.

REMEDIATION

1. Ensure to update Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS) to latest version 9.1R8 or higher.

2. Ensure to check & fix misconfiguration issues in Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS).

INTRODUCTION

Multiple vulnerabilities in Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS) can be taken advantage by attackers in hacking campaign.

Google TOTP authentication bypass vulnerability (CVE-2020-8206), arbitrary code execution vulnerability (CVE-2020-8218), read arbitrary files vulnerability (CVE-2020-8221), and unauthorized root access vulnerability (CVE-2020-12880) in Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS) poses a severe risk of security breach followed by data breach incident.

In attack scenario, attacker would first target Google TOTP authentication bypass vulnerability (CVE-2020-8206) after obtaining login credentials using social engineering attack like phishing or spear-phishing email sent to the target of interest. After initial unauthorized access, attacker would subsequently trigger either of these three vulnerabilities (CVE-2020-8218, CVE-2020-8221, CVE-2020-12880) depending on the end goals (or intentions). Incase of intention like malware delivery, attacker would think of exploiting arbitrary code execution vulnerability (CVE-2020-8218). Incase of intention like data breach or gain further access, attacker would think of exploiting read arbitrary files vulnerability (CVE-2020-8221) and unauthorized root access vulnerability (CVE-2020-12880).

The business impact that these vulnerabilities might cause are, unauthorized access, data breach, security breach, breach of customer trust, disruption in business operations, and may impact reputation of an organization.

AFFECTED PRODUCTS

- Pulse Connect Secure (PCS) versions prior to 9.1R8
- Pulse Policy Secure (PPS) versions prior to 9.1R8

READ

- SA44516 - 2020-07: Security Bulletin: Multiple Vulnerabilities Resolved in Pulse Connect Secure / Pulse Policy Secure 9.1R8

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

3rd August 2020 – 13th August 2020 | TRAC-ID: NII20.08.0.2

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
August 13, 2020	Ubuntu Linux	USN-4459-1: Salt vulnerabilities	▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS	Security Patch Update
August 13, 2020	Ubuntu Linux	USN-4458-1: Apache HTTP Server vulnerabilities	▪ Ubuntu 20.04 LTS ▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS	Security Patch Update
August 12, 2020	Ubuntu Linux	USN-4457-1: Software Properties vulnerability	▪ Ubuntu 20.04 LTS ▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS	Security Patch Update

REDHAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
August 12, 2020	Red Hat Enterprise Linux	RHSA-2020:3433	▪ Red Hat Enterprise Linux Server - AUS 7.4 x86_64 ▪ Red Hat Enterprise Linux Server - TUS 7.4 x86_64	Security Patch Update
August 12, 2020	Red Hat Enterprise Linux	RHSA-2020:3432	▪ Red Hat Enterprise Linux Server - AUS 7.4 x86_64 ▪ Red Hat Enterprise Linux Server - TUS 7.4 x86_64	Security Patch Update
August 11, 2020	Red Hat Enterprise Linux	RHSA-2020:3422	▪ 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	Security Patch Update

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

3rd August 2020 – 13th August 2020 | TRAC-ID: NII20.08.0.2

August 10, 2020	**Red Hat Enterprise Linux**	RHSA-2020:3386	▪ Red Hat Enterprise Linux for x86_64 8 x86_64 ▪ Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.2 x86_64	Security Patch Update
August 10, 2020	**Red Hat Enterprise Linux**	RHSA-2020:3385	▪ 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	Security Patch Update
August 10, 2020	**Red Hat JBoss Enterprise Application**	RHSA-2020:3382	▪ JBoss Enterprise Application Platform Text-Only Advisories x86_64	Security Patch Update

IBM

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
August 13, 2020	**IBM WebSphere Service Registry and Repository**	Multiple vulnerabilities in IBM® Java SDK affect WebSphere Service Registry and Repository and WebSphere Service Registry and Repository Studio July 2020 CPU plus deferred CVE-2019-2590 and CVE-2020-2601	▪ IBM WebSphere Service Registry and Repository V8.5 ▪ IBM WebSphere Service Registry and Repository Studio V8.5	Kindly update to fixed version
August 13, 2020	**IBM WebSphere Application Server**	WebSphere Application Server is vulnerable to a remote code execution vulnerability (CVE-2020-4589)	▪ WebSphere Application Server 9.0 ▪ WebSphere Application Server 8.5 ▪ WebSphere Application Server 8.0 ▪ WebSphere Application Server 7.0	Kindly update to fixed version