NETWORK INTELLIGENCE

The Digital Security Company

May 2023, Edition 1.0

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- Team Insane PK is widely targeting Indian Banking & Finance websites with DDoS attacks
- ChatGPT suffered a data leak incident due to an open-source bug
- Multiple critical vulnerabilities in Cisco Small Business Series Switches
- CVE-2023-28929: A DLL hijacking vulnerability in Trend Micro Security & OfficeScan Cloud

Also Inside

Security Patch Advisory

Critical High Low

Date: May 24, 2023

Team Insane PK is widely targeting Indian Banking & Finance websites with DDoS attacks

RECOMMENDATIONS

1. Prioritize remediating known exploited vulnerabilities.

2. Implement Anti-DDoS measures on both On-premise and cloud for real-time DDoS attack prevention.

3. Utilize content delivery networks (CDNs) to distribute traffic.

4. Implement bot-detection technologies and algorithms -to identify large-scale web requests from botnets employed by actors to conduct DDOS Attacks.

5. Make sure your sites' infrastructure is up to date with the latest patches. If you're using WordPress, make sure plugins and themes are updated as well.

6. Scan your site for vulnerabilities to verify no patches are missing.

7. Make sure your WAF service/appliance is updated with the latest signatures. If possible, enable geolocation and restrict traffic to valid locations.

8. If possible, implement IP address access control lists (ACLs) in order to restrict access to Internet-facing systems.

9. Ensure MySQL server, Apache HTTP server, Apache Tomcat server, Confluence Server and Data Center are updated with latest security patches.

10.Use strong passwords and enforce multifactor authentication wherever possible.
11.Monitor child processes of web application processes for suspicious processes.

12.Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs.

INTRODUCTION

Team_Insane_Pk is a notorious hacktivist gang from Pakistan that has been active since July 2022. The hacktivist group is widely targeting Iran under #OpIran & India under #OpIndia in DDoS operations.

On May 16, Team_Insane_Pk claimed to have taken down 44 Indian banking and finance websites (Private, Government and Public) via DDoS attacks on its Telegram channel. Also, on the same day, the group claimed to have takedown 23 Indian police websites.

The DDoS attacks launched by the hacktivist group disrupted crucial government infrastructure and impacted the citizen's ability to interact with the respective banks and with the police.

The hacktivist group states the attacks were launched in retaliation to the cyber warfare occurring between Indian hacktivist teams like team UCC operations, Indian Cyber Force, and CyberXForce, and hacktivist teams belonging to Pakistan and Malaysia.

REFERENCES

1. Team Insane PK claims DDoS Attack on 44 Indian Banking and Finance Websites

SECURITY ADVISORY

Date: May 23, 2023

ChatGPT suffered a data leak incident due to an open-source bug

RECOMMENDATIONS

1. Provide awareness among employees and management staffs to not accidentally upload or leak sensitive information on AI chatbot platforms such as ChatGPT. Exposure of personal data can have serious consequences, including identity theft and financial fraud.

2. If possible, limit the length of questions submitted to ChatGPT.

3. It is strongly recommended to provide guidance for customers on identifying and avoiding fraudulent emails, websites, and calls, and urge them to immediately report any suspicious activities to the bank.

4. Stay vigilant on all your account activities. Sign up for SMS and email alerts that can raise red flags in case of suspicious activity.

5. Ensure to be more vigilant while communicating over email or phone call, to eliminate risk of social engineering like phishing.

6. Pay close attention to false sense of urgency, electronic communications impersonating one of the company's vendors, requests for wire transfers.

INCIDENT BRIEFING

OpenAI says it fixed a bug in the ChatGPT AI chatbot that caused a small number of users to view other users' titles and past conversations. The issue came to light after ChatGPT users posted images of other people's conversations on social media.

The data leak incident also exposed information such as subscribers' names, email addresses, payment addresses, and the last four digits of their credit card number and expiration date.

OpenAI CEO Sam Altman blamed the issue on "a bug in an open-source library." The bug existed in the Asyncio redis-py client for Redis Cluster and has now been fixed.

LESSON LEARNED

- Lack of timely and informed cyber security awareness among employees and management staff, might lead accidentally uploading and leaking of confidential data on platforms such as ChatGPT, Bard, or other similar Large Language Models (LLMs).
- The incident highlights the importance of cybersecurity measures and the need for companies to take all necessary steps to protect their customers' data.

REFERENCES

- OpenAI: ChatGPT payment data leak caused by open-source bug
- OpenAI Confirms ChatGPT Data Breach

SECURITY ADVISORY

Date: May 18, 2023

Multiple critical vulnerabilities in Cisco Small Business Series Switches

BUSINESS IMPACT

Successful exploitation allows unauthenticated attackers to execute arbitrary code with root privileges, cause a DoS condition or read unauthorized information from vulnerable devices.

RECOMMENDATIONS

1. Update 250 Series Smart Switches, 350 Series Managed Switches, 350X Series Stackable Managed Switches, and 550X Series Stackable Managed Switches to firmware version 2.5.9.16 or above.

2. Update Business 250 Series Smart Switches and Business 350 Series Managed Switches to firmware version 3.3.0.16 or above.

To download the firmware from the Software Center on Cisco.com, click Browse all and choose Switches > LAN Switches - Small Business.

REFERENCES

1. Cisco warns of critical switch bugs with public exploit code
2. Cisco Small Business Series Switches Buffer Overflow Vulnerabilities

INTRODUCTION

Cisco has addressed multiple vulnerabilities existing in the web-based user interface of certain Cisco Small Business Series Switches.

The vulnerabilities are tracked as CVE-2023-20024 (CVSS Score: 8.6), CVE-2023- 20156 (CVSS Score: 8.6), CVE-2023-20157 (CVSS Score: 8.6), CVE-2023-20158 (CVSS Score: 8.6), CVE-2023-20159 (CVSS Score: 9.8), CVE-2023-20160 (CVSS Score: 9.8), CVE-2023-20161 (CVSS Score: 9.8), CVE-2023-20162 (CVSS Score: 7.5) & CVE-2023-20189 (CVSS Score: 9.8).

The vulnerabilities exist due to improper validation of requests that are sent to the web interface. An attacker could exploit this vulnerability by sending a crafted request through the web-based user interface in low-complexity attacks that don't require user interaction.

Cisco has warned that proof-of-concept exploit code is available for these vulnerabilities.

AFFECTED PRODUCTS

The vulnerabilities affect the following Cisco Small Business Switches if they are running a vulnerable firmware release:

- 250 Series Smart Switches
- 350 Series Managed Switches •
- 350X Series Stackable Managed Switches
- 550X Series Stackable Managed Switches
- Business 250 Series Smart Switches
- Business 350 Series Managed Switches
- Small Business 200 Series Smart Switches
- Small Business 300 Series Managed Switches
- Small Business 500 Series Stackable Managed Switches

➢ For 250 Series Smart Switches, 350 Series Managed Switches, 350X Series Stackable Managed Switches, and 550X Series Stackable Managed Switches: Vulnerable Cisco Firmware Releases - 2.5.9.15 and earlier.

➢ For Business 250 Series Smart Switches and Business 350 Series Managed Switches: Vulnerable Cisco Firmware Releases - 3.3.0.15 and earlier.

NOTE: Cisco states that the Small Business 200 Series Smart Switches, Small Business 300 Series Managed Switches, and Small Business 500 Series Stackable Managed Switches will not be patched because these devices have entered the end-of-life process. Date: 18th May 2023 NETWORK INTELLIGENC

SECURITY ADVISORY

Date: May 3, 2023

CVE-2023-28929: A DLL hijacking vulnerability in Trend Micro Security & OfficeScan Cloud

BUSINESS IMPACT

Successful exploitation of the vulnerability enables threat actors to bypass security, execute arbitrary programs with administrative privileges, allow DLL hijacking even for third-party applications that do not have vulnerabilities and plant further malware on an organization's critical systems and endpoints

INTRODUCTION

Trend Micro has released fixes to address the CVE-2023-28929 bug in Trend Micro Security for Windows family & OfficeScan Cloud antivirus engine.

CVE-2023-28929 (CVSS Score: 7.8) is a DLL hijacking vulnerability that exists because the vulnerable application loads DLL libraries in an insecure manner.

A remote attacker can place a malicious .dll on a remote SMB file share, trick the victim into opening a specially crafted executable file and execute arbitrary code on the victim's system.

RECOMMENDATIONS

1. Update Trend Micro Security for Windows to 2022/2023 (17.7.1634 and above)
2. Update Trend Micro Security for Windows to 2021 (17.0.1426 and above)
3. Ensure TrendMicro's OfficeScan antivirus engine is running versions 17.7.1476 and above or 17.0.1428 and above

AFFECTED PRODUCTS

- Trend Micro Security: 2022/2023 (17.7.1476 and below)
- Trend Micro Security: 2021 (17.0.1412 and below)
- OfficeScan Cloud versions before 17.7.1476
- OfficeScan Cloud versions before 17.0.1428

REFERENCES

1. Security Bulletin: Trend Micro Security DLL Hijacking
2. Reported OfficeScan Vulnerability (CVE-2023-28929)

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

22nd May 2023 – 28th May 2023
TRAC-ID: NII23.05.0.4

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	USN-6073-9: osbrick regression	• Ubuntu 23.04 • Ubuntu 22.10 • Ubuntu 22.04 LTS • Ubuntu 20.04 LTS	Kindly update to fixed version
Ubuntu Linux	USN-6073-8: Nova regression	• Ubuntu 23.04 • Ubuntu 22.10 • Ubuntu 22.04 LTS • Ubuntu 20.04 LTS	Kindly update to fixed version

F5 NETWORKS

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Traffix SDC	K000134768: Linux kernel vulnerability CVE-2022-4378	• Traffix SDC: 5.1.0	Kindly update to fixed version
Traffix SDC	K000134770: Linux kernel vulnerability CVE-2022-42703	• Traffix SDC: 5.2.0 - 5.2.4, 5.1.0	Kindly update to fixed version

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

22nd May 2023 – 28th May 2023
TRAC-ID: NII23.05.0.4

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2023-3082	• Oracle Linux 8 (aarch64) • Oracle Linux 8 (x86_64	**Kindly update to fixed version**
Oracle Linux	ELSA-2023- 12354	• Oracle Linux 8 (x86_64)	**Kindly update to fixed version**

VMWARE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
NSX-T	**NSX-T update addresses cross-site scripting vulnerability (CVE-2023-20868)**	• NSX-T versions 3.2.x • Cloud Foundation (NSX-T) versions 4.5.x	**Kindly update to fixed version**

SECURITY ADVISORY