NETWORK INTELLIGENCE
The Digital Security Company

November 2022, Edition 1.0

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- 🔴 Critical Pre-Auth RCE bug in the Oracle Access Manager
- 🔴 Twitter's massive data leak has impacted more than 5.4 million users
- 🔴 AirAsia suffered a data breach incident due to a ransomware attack by Daixin Team
- 🔴 Multiple vulnerabilities in VMware Workspace ONE Assist

Also Inside

Security Patch Advisory

🔴 Critical 🟡 High 🟢 Low

Date: November 30, 2022

Critical Pre-Auth RCE bug in the Oracle Access Manager

BUSINESS IMPACT

Successful exploitation of vulnerability enables an attacker to completely compromise and take over Access Manager instances to create any user with any privileges or execute arbitrary code in the victim's server

RECOMMENDATIONS

1. Ensure Oracle Access Manager is updated to the latest version.

INTRODUCTION

A critical pre-auth RCE vulnerability (tracked as CVE-2021-35587) impacting the Oracle Access Manager (OAM) product of Oracle Fusion Middleware is currently under active exploitation.

The vulnerability exists due to improper input validation within the OpenSSO Agent component in Oracle Access Manager. A remote non-authenticated attacker with network access via HTTP can exploit this vulnerability to take over the OAM server and execute arbitrary code.

- CVSS Score: 9.8

AFFECTED PRODUCTS

- OAM versions 11.1.2.3.0, 12.2.1.3.0, and 12.2.1.4.0

REFERENCES

- CISA Warns of Actively Exploited Critical Oracle Fusion Middleware Vulnerability
- CISA adds Oracle Fusion Middleware flaw to its Known Exploited Vulnerabilities Catalog

Date: November 29, 2022

Twitter's massive data leak has impacted more than 5.4 million users

RECOMMENDATIONS

1. Keep all operating systems and software up to date. Prioritize patching known exploited vulnerabilities.

2. Ensure to have a decent Antivirus program installed on computer.

3. Ensure to assess & resolve data scraping flaws and implement anti-scraping measures to mitigate unauthorized data mining and data scraping.

4. Enhance data security and data privacy controls.

5. Adhere to data sharing and data governance practices.

6. Ensure to be more vigilant while communicating over email or phone call, to eliminate risk of social engineering like spam/phishing/identity theft attacks.

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

8. Enable app-based multi-factor authentication to mitigate potential access to bank accounts by hackers due to SIMswap attacks.

9. Rate limit API and controller access to minimize the harm from automated attack tooling.

10.Control MFA push with features such as number matching to improve user sign-in security. (Ex: Number matching in Azure MFA and number matching in Duo called

INCIDENT BRIEFING

Twitter has suffered a massive data breach by multiple threat actors due to an API vulnerability in its platform.

The vulnerability allowed attackers without authentication to obtain a Twitter ID of any user by submitting a phone number/email even though the user has prohibited this action in the privacy settings. The bug exists due to an issue in the authorization process used in the Android Client of Twitter, specifically in the process of checking the duplication of a Twitter account.

The security issue allowed threat actors to scrape public information (such as Twitter ID, name, screen name, verified status, location, URL, description, follower count, account creation date, friends count, favourites count, statuses count, and profile image URLs) as well as non-public information (such as phone numbers and email addresses).

In July 2022, a threat actor known as 'Devil' was selling the allegedly stolen data for $30,000, which was later purchased by two different threat actors. Twitter confirmed the data breach incident in August 2022. It stated that threat actors exploited a zeroday vulnerability reported by HackerOne in December 2021 and fixed by them in January 2022.

On November 24th, 2022, a threat actor known as 'GOD' was spotted selling the 5.4 million Twitter records for free on a hacking forum.

Additionally, a security expert named Chad Loder disclosed another larger Twitter data dump affecting millions of Twitter accounts in the EU and US that was only shared privately among a few people. The data sample file leaked contains information of 1.4 million Twitter profiles for suspended users. This newly discovered data dump consists of numerous files broken up by country and area codes, including Europe, Israel, and the USA.

This data leak incident more likely leads to a loss of privacy for many users.

LESSON LEARNED

Vulnerability or misconfiguration issue in software and inadequate security control often allows attackers to gain initial foothold onto the system or network, exfiltrate sensitive data and cause further damages to cloud-based or on-premises IT Infrastructure.

REFERENCES

- 5.4 million Twitter users' stolen data leaked online — more shared privately
- Data from 5.4M Twitter users obtained from multiple threat actors and combined with data from other breaches

SECURITY ADVISORY

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

Date: November 21, 2022

AirAsia suffered a data breach incident due to a ransomware attack by Daixin Team

RECOMMENDATIONS

1. Ensure all operating systems and software are up to date. Prioritize patching known exploited vulnerabilities.
2. Refrain from opening untrusted links and email attachments without verifying their authenticity.
3. Turn off SSH and other network device management interfaces such as Telnet, Winbox, and HTTP for wide area networks (WANs) and secure with strong passwords and encryption when enabled.
4. Enable multi-factor authentication if its currently not in use and use secure MFA method, such as a hardware security key or an authentication app.
5. Use solutions that support Fast ID Online (FIDO) v2.0 and certificate-based authentication.
6. Use conditional access policies to prevent from attacks that leverage stolen credentials and session cookie by enabling policies such as compliant devices or trusted IP address requirements.
7. Continuously monitor for suspicious sign-in attempts with suspicious characteristics (for example, location, ISP, user agent, use of anonymizer services).
8. Monitor for unusual mailbox activities such as the creation of Inbox rules with suspicious purposes or unusual amounts of mail item access events by untrusted IP addresses or devices.
9. Stay vigilant on all your account activities. Sign up for SMS and email alerts that can raise red flags in case of suspicious activity.
10. Check the online banking site URL for HTTPS protocol and ensure that the URL is correctly spelled.
11. Control MFA push with features such as number matching to improve user sign-in security. (Ex: Number matching in Azure MFA and number matching in Duo called Duo Verified Push)
12. Configure user email alerts for new MFA and MDM device enrolments. Configure alert on volume of push attempts per account.

INCIDENT BRIEFING

Capital A Berhad, operating as AirAsia, is a Malaysian multinational low-cost airline headquartered near Kuala Lumpur, Malaysia. It is the largest airline in Malaysia by fleet size and destinations.

AirAsia Group was allegedly hit by the Daixin ransomware group on November 11 and 12. Daixin Team claim that they obtained the personal data of 5 million unique passengers and all employees.

The sample files leaked by Daixin Team contained passengers' and employees' personal information such as name, date of birth, country of birth, location, date employment started, their "secret question," "answer," and salt. The threat actor group stated that they plan to make information about the AirAsia network, including backdoors, available privately and freely on hacker forums.

- Daixin actors are observed using stolen credentials or exploiting vulnerabilities in the organization's VPN server to gain initial access.
- Post initial access, Daixin actors move laterally via SSH & RDP and gain privileged account access through credential dumping & pass the hash.
- Next, the attackers are observed leveraging privileged accounts to gain access to VMware vCenter Servers and ESXi servers and deploy ransomware.
- The actors used Rclone and Ngrok tools for data exfiltration. The encrypted files are appended with the following extensions: .vmdk, .vmem, .vswp, .vmsd, .vmx, and .vmsn.

LESSON LEARNED

Lack of endpoint security, use of admin account, using unpatched operating system, usage of commonly used passwords, reuse of same passwords across different platforms and failed to comply with security practices, often allows attackers to gain initial access onto the organization network and cause further damage.

REFERENCES

- AirAsia victim of ransomware attack, passenger & employee data acquired
- Daixin Team

SECURITY ADVISORY

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

Date: November 09, 2022

Multiple vulnerabilities in VMware Workspace ONE Assist

BUSINESS IMPACT

Successful exploitation of the vulnerabilities may allow a remote attacker to bypass authentication and elevate privileges to admin, steal potentially sensitive information, change the appearance of the web page, and perform XSS, phishing and drive-by-download attacks

RECOMMENDATIONS

1. Ensure to update Workspace ONE Assist for Windows to the latest version.

INTRODUCTION

VMware has released security updates to address a trio of critical-rated flaws in Workspace ONE Assist for Windows – a product used by IT and help desk staff to remotely take over and manage employees' devices. A threat actor able to reach a Workspace ONE Assist deployment, either over the internet or on the network, can exploit any of these three bugs to obtain administrative access without the need to authenticate. The three flaws (tracked as CVE2022-31685, CVE-2022-31686 & CVE-2022-31687) are all rated 9.8 out of 10 in CVSS severity.

Authentication Bypass Vulnerability (CVE-2022-31685) exists due to an error when processing authentication requests, Broken Authentication Method vulnerability (CVE-2022-31686) exists due to an error in the authentication method and Broken Access Control vulnerability (CVE-2022-31687) exists due to improper access restrictions. A remote non-authenticated attacker with network access to Workspace ONE Assist can bypass the authentication process and implemented security restrictions to obtain administrative access to the system.

VMware has also addressed a reflected XSS vulnerability (CVE-2022-31688) that enables attackers to inject & run JavaScript code in the target user's window and a session fixation vulnerability (CVE-2022-31689) that allows attackers to authenticate to the application after obtaining a valid session token.

AFFECTED PRODUCTS

- VMware Workspace ONE Assist for Windows versions 21.x and 22.x

REFERENCES

- VMware fixes three critical auth bypass bugs in remote access tool
- VMware Workspace ONE Assist update addresses multiple vulnerabilities

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

14th Nov 2022 – 20th Nov 2022
TRAC-ID: NII22.11.0.3

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	**USN-5723-1: Vim vulnerabilities**	• Ubuntu 16.04 ESM	**Kindly update to fixed version**
Ubuntu Linux	**USN-5625-2: Mako vulnerability**	• Ubuntu 22.10	**Kindly update to fixed version**

SUSE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
SUSE Linux	**SUSE-SU2022:4080-1**	• SUSE Linux Enterprise Server 12-SP5	**Kindly update to fixed version**
SUSE Linux	**SUSE-SU2022:4075-1**	• SUSE OpenStack Cloud Crowbar 8 • SUSE OpenStack Cloud Crowbar 9	**Kindly update to fixed version**

SECURITY ADVISORY

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

14th Nov 2022 – 20th Nov 2022
TRAC-ID: NII22.11.0.3

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2022-7928	• Oracle Linux 8 (aarch64) • • Oracle Linux 8 (x86_64)	Kindly update to fixed version
Oracle Linux	ELSA-2022-7826	• Oracle Linux 8 (aarch64) • Oracle Linux 8 (x86_64	Kindly update to fixed version

CISCO

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Cisco ISE	Cisco Identity Services Engine Vulnerabilities	• Cisco ISE ReleaseS: 2.7 and earlier, 3.0 and earlier, 3.1, 3.2	Kindly update to fixed version

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com