NETWORK INTELLIGENCE

The Digital Security Company

January 2024, Edition

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- Massive Data Breach: Personal Data of 750 Million Indians Allegedly Up for Sale.
- Midnight Blizzard Chronicles: A Deep Dive into the NOBELIUM Cyber Threat.
- Unmasking the Exploitation of Google OAuth2 for Persistent Account Access.
- Ivanti Resolves Critical RCE Bug in Endpoint Management Software.

Also Inside

Security Patch Advisory

Critical High Low

Date: Jan 29, 2024

Massive Data Breach: Personal Data of 750 Million Indians Allegedly Up for Sale

RECOMMENDATIONS

1. Keep all software up to date and prioritize patching to known exploited vulnerabilities (KEVs).

2. Ensure compliance with data protection regulations to mitigate legal and financial repercussions associated with data breaches.

3. Conduct awareness programs to educate users about potential scams and phishing attempts, emphasizing vigilance in online interactions.

4. Enforce the use of multi-factor authentication for all user accounts to add an additional layer of security beyond passwords.

5. Implement the principle of least privilege by restricting access permissions based on job roles and responsibilities. Regularly review and update access controls.

6. Implement strong encryption protocols for sensitive data, both in transit and at rest, to prevent unauthorized access even if a breach occurs.

7. Conduct regular tabletop exercises to simulate cybersecurity incidents and test the effectiveness of the incident response plan.

INCIDENT BRIEFING

Researchers at CloudSEK disclosed of a massive Indian Mobile Network Consumer Database for sale by CYBO CREW affiliates for $3,000.

While this breach incident was spotted by CloudSEK on January 23 via a post by a threat actor known as CyboDevil on an underground forum, a similar database was offered for sale on January 14 by another threat actor named UNIT8200 via Telegram.

The threat actor claims to have stolen 1.8TB of data, which includes information such as names, mobile numbers, addresses, and Aadhaar details of 750 million individuals.

While the exact method of data breach remains unclear, the report hints at the likely exploitation of vulnerabilities within government databases or telecommunication systems.

CyboDevil and UNIT8200, affiliates of the CYBOCREW group, active since July 2023, have previously breached multiple organizations in the automobile, jewellery, insurance, and apparel sectors.

The data exposed in the breach incident is more likely to be abused in financial fraud, social engineering tactics, identity theft, and targeted scam campaigns.

LESSON LEARNED

- The incident highlights the urgency of addressing systemic weaknesses, collaborating with relevant authorities, and implementing robust cybersecurity measures to safeguard against unauthorized access and data breaches.

REFERENCES

1. Aadhaar details, phone numbers of nearly 75 crore Indians put up for sale, claims cybersecurity firm
2. 1.8TB Indian Mobile Network Consumer Database of 750 Million Individuals Up for Sale by Threat Actors

SECURITY ADVISORY

Date: Jan 29, 2024

Midnight Blizzard Chronicles: A Deep Dive into the NOBELIUM Cyber Threat

RECOMMENDATIONS

1. Eliminate insecure passwords. Enforce the use of MFA for all user accounts. Educate users to review sign-in activity and mark suspicious sign-in attempts as “This wasn’t me”.

2. Midnight Blizzard has also been known to abuse OAuth applications in past attacks against other organizations using the EWS.AccessAsUser.All Microsoft Graph API role or the Exchange Online ApplicationImpersonation role to enable access to email. Defenders are recommended to review any applications that hold EWS.AccessAsUser.All and EWS.full_access_as_app permissions and understand whether they are still required in your tenant. If they are no longer required, they should be removed.

3. If you require applications to access mailboxes, granular and scalable access can be implemented using role-based access control for applications in Exchange Online. This access model ensures applications are only granted to the specific mailboxes required.

4. Audit identities that hold ApplicationImpersonation privileges in Exchange Online. ApplicationImpersonation allows a caller, such as a service principal, to impersonate a user and perform the same operations that the user themselves could perform.

5. Conduct regular security audits and configuration reviews, especially for accounts with elevated privileges, test accounts or legacy systems, to identify and rectify potential weaknesses.

INTRODUCTION

On January 25, Microsoft published a technical report detailing how Midnight Blizzard actors gained access to its corporate email servers after password-spraying a legacy non-production test tenant account lacking MFA last November.

Midnight Blizzard, attributed to the Russian Foreign Intelligence Service (SVR), specializes in espionage, targeting governments, diplomatic entities, NGOs, and IT service providers primarily in the US and Europe. As per Microsoft, hackers leveraged the test account to further compromise a legacy test OAuth application and gain elevated access to the Microsoft corporate environment.

Next, the actors created additional malicious OAuth applications. They used legacy test OAuth application to grant them Office 365 Exchange Online full_access_as_app role to obtain access to mailboxes of Microsoft corporate email accounts.

Midnight Blizzard actors also employed residential proxy networks to route their traffic through numerous IP addresses commonly used by legitimate users. This strategy allowed them to interact with compromised systems, including Exchange Online, while evading traditional indicators of compromise.

REFERENCES

1. Microsoft Warns of Widening APT29 Espionage Attacks Targeting Global Orgs
2. Microsoft reveals how hackers breached its Exchange Online accounts
3. Midnight Blizzard: Guidance for responders on nation-state attack

SECURITY ADVISORY

Date: Jan 16, 2024

Unmasking the Exploitation of Google OAuth2 for Persistent Account Access

RECOMMENDATIONS

1. This exploit remains effective even after users have reset their passwords. Hence, changing the password alone is not sufficient. If you suspect your account may have been compromised, or as a general precaution, sign out of all browser profiles to invalidate the current session tokens. Following this, reset your password and sign back in to generate new tokens.

Administrators managing Google Accounts for a company, school, or other group can sign a user out of a managed Google Account, such as Google Workspace or Cloud Identity and reset a user's sign-in cookies via below steps:

• Sign in to your Google Admin console. Sign in using an administrator account, not your current account.
• In the Admin console, go to Menu > Directory > Users. • In the Users list, find the user. If you need help, go to Find a user account.
• Click the user's name to open the user's account page.
• Click Security > Sign-in cookies > Reset.

2. To check whether someone has accessed your account, you can view which computers, phones, or other devices that were signed into your Google Account recently.

Go to your Google Account -> Security -> Manage all devices.

3. To protect accounts users are advised to regularly check for unfamiliar sessions, change passwords, and be vigilant while downloading unknown software, unknown attachments.

INTRODUCTION

In the latest blog post, CloudSEK unveiled a severe exploit that enables the generation of persistent Google cookies through token manipulation.

The exploit was initially disclosed on a Telegram channel by a threat actor named 'PRISMA' on 20 October 2023. The threat actor advertised two key features, i.e., Session Persistence and Cookie Generation.

The exploit's root was identified as an undocumented Google OAuth endpoint named "MultiLogin," presenting significant cybersecurity concerns. This endpoint operates by accepting a vector of account IDs and auth-login tokens.

Currently, this exploit is incorporated in malware such as Lumma, Rhadamanthys, Risepro, Meduza, White Snake and Stealc Stealer.

The malwares target Chrome's token_service table of WebData to extract tokens and account IDs of chrome profiles logged in. The token_service table contains GAIA ID and encrypted_token, which can be decrypted via encryption keys stored in Chrome's Local State.

Next, the malwares manipulate token:GAIA ID pair which when used in conjunction with the MultiLogin endpoint, enables the regeneration of expired Google Service cookies and maintain persistent access on compromised accounts.

REFERENCES

1. Malware abuses Google OAuth endpoint to 'revive' cookies, hijack accounts
2. Compromising Google Accounts: Malwares Exploiting Undocumented OAuth2 Functionality for session hijacking
3. Google: Malware abusing API is standard token theft, not an API issue
4. Info-stealers can steal cookies for permanent access to your Google account

SECURITY ADVISORY

Date: Jan 05, 2024

Ivanti Resolves Critical RCE Bug in Endpoint Management Software

IMPACT

Successful exploitation of the vulnerability poses a significant risk by enabling unauthenticated attackers to hijack enrolled devices or compromise the core server.

RECOMMENDATIONS

1. Ensure to update Ivanti Endpoint Manager to EPM 2022 SU5 or above.

INTRODUCTION

On January 04, Ivanti released fixes to address a critical remote code execution vulnerability (CVE-2023-39336; CVSS Score: 9.6) in its Endpoint Management software (EPM).

The flaw enables an attacker with access to the internal network to execute arbitrary SQL queries through an unspecified SQL injection weakness and gain control over machines running the EPM agent. In cases where the core server was configured to use SQL Express, this could lead to remote code execution on the core server.

The vulnerability is more likely to be exploited in targeted hacking campaigns and malware attacks due to low attack complexity and no special privileges or user interaction requirements.

AFFECTED PRODUCTS

- Ivanti EPM 2021/EPM 2022 prior to SU5

REFERENCES

1. Ivanti warns critical EPM bug lets hackers hijack enrolled devices
2. SA-2023-12-19-CVE-2023-39336

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

15th Jan 2024 – 21st Jan 2024
TRAC-ID: NII24.01.0.3

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	USN-6590-1: Xerces-C++ vulnerabilities	• Ubuntu 22.04 LTS • Ubuntu 20.04 LTS • Ubuntu 18.04 ESM • Ubuntu 16.04 ESM • Ubuntu 14.04 ESM	Kindly update to fixed version
Ubuntu Linux	USN-6589-1: FileZilla vulnerability	• Ubuntu 23.10 • Ubuntu 22.04 LTS • Ubuntu 20.04 LTS	Kindly update to fixed version

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2024-0248	• Oracle Linux 8 (aarch64) • Oracle Linux 8 (x86_64)	Kindly update to fixed version
Oracle Linux	ELSA-2024-0249	• Oracle Linux 9 (aarch64) • Oracle Linux 9 (x86_64)	Kindly update to fixed version

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

15th Jan 2024 – 21st Jan 2024
TRAC-ID: NII24.01.0.3

IBM

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
IBM® Db2®	Multiple vulnerabilities in IBM Java SDK and IBM Java Runtime affect IBM® Db2®. (Oct 2023 CPU)	• IBM® Db2® 10.5.0.x • IBM® Db2® 11.1.4.x • IBM® Db2® 11.5.x	**Kindly update to fixed version**
IBM AIX and VIOS	Security Bulletin: AIX is vulnerable to cache poisoning due to ISC BIND (CVE-2021-25220)	• AIX 7.1 • AIX 7.2 • AIX 7.3 • VIOS 3.1	**Kindly update to fixed version**

GOOGLE CHROME

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Chrome	**Chrome for Android Update**	• Chrome versions prior to 121.0.6167.71 for Android	**Kindly update to fixed version**

SECURITY ADVISORY