NETWORK INTELLIGENCE

The Digital Security Company

November 2023, Edition

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- DeleFriend – a design flaw in Google Workspace's Domain-Wide delegation feature.
- CVE-2023-6345 – A new 0-day bug in Google Chrome actively exploited in attacks.
- Vulnerabilities in fingerprint sensors can enable hackers to bypass Windows Hello authentication.
- The Intricate Puzzle of the LinkedIn Database 2023: Fact or Fiction?

Also Inside

Security Patch Advisory

Critical High Low

Date: Nov 30, 2023

DeleFriend – a design flaw in Google Workspace's Domain-Wide delegation feature

RECOMMENDATIONS

1. Smartly manage roles for GCP resources with Domain-Wide delegation, ensuring only necessary IAM users have permission to create private keys on sensitive service accounts. Ideally, create each service account in a separate project if possible.

2. Limit OAuth scopes in delegations as much as possible. Adhere to the principle of least privilege, where an application only requests permissions it absolutely needs.

3. Also, refrain from using administrative scopes such as https://www.googleapis.com/auth/admin to minimize potential impact in case of a compromise.

INTRODUCTION

Hunters' Team Axon researchers discovered a design flaw named DeleFriend in Google Workspace's Domain-Wide delegation (DWD) feature and released a proof-of-concept red team tool that can abuse this feature to access Workspace user data via Google Cloud Platform (GCP) service accounts.

DWD feature enables GCP identity objects to execute tasks on Google SaaS applications, such as Gmail, Google Calendar, Google Drive, and more, on behalf of other Workspace users.

Researchers disclosed two scenarios of abusing the Domain-Wide delegation feature.

In the first scenario, the Domain-Wide delegation feature is abused as a post-exploitation technique to achieve robust persistence and capabilities for exfiltration. Prerequisites include a threat actor gaining initial access to an IAM identity, having the ability to create service accounts in a GCP project, and obtaining super admin privileges to GWS. The attack steps include creating a new service account and corresponding key pair on GCP and establishing a new delegation rule for the service account resource. The second scenario abuses existing delegations in the GCP and Google Workspace without possessing super admin privileges. The prerequisite includes the threat actor gaining initial access to an IAM identity and having the ability to create new private keys to a relevant GCP service account resource that has existing domain-wide delegation permissions. Actors can use the DeleFriend POC tool to automate, find, and abuse existing delegation between GCP and GWS.

Successful abuse could result in the theft of emails from Gmail, data exfiltration from Google Drive, or other unauthorized actions within Google Workspace APIs on all the identities in the target domain.

REFERENCES

- Design Flaw in Google Workspace Could Let Attackers Gain Unauthorized Access
- DeleFriend: Severe design flaw in Domain Wide Delegation could leave Google Workspace vulnerable for takeover

SECURITY ADVISORY

Date: Nov 29, 2023

CVE-2023-6345 – A new 0-day bug in Google Chrome actively exploited in attacks.

IMPACT

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code, bypass security restrictions, crash the Chrome app or plant spyware on the targeted system

RECOMMENDATIONS

1. Kindly update Microsoft Exchange servers to the latest versions as soon as patches are released.

2. Implementing multi-factor authentication is strongly advised to prevent cybercriminals from accessing Exchange instances even when account credentials have been compromised.

INCIDENT BRIEFING

Google has released updates to its Chrome browser for Windows, Mac, Linux, and Android to address 7 security issues.

These vulnerabilities are tracked as CVE-2023-6348, CVE-2023-6347, CVE2023-6346, CVE-2023-6350, CVE-2023-6351 and CVE-2023-6345.

These vulnerabilities exist in Google Chrome due to:
• Type Confusion in Spellcheck.
• Use after free in Mojo, WebAudio and libavif.
• Out-of-bounds memory access in libavif.
• Integer overflow in Skia.

A remote attacker can trick the victim into opening a specially crafted web page, trigger type confusion, out-of-bounds memory access, integer overflow or use-after-free errors, and execute arbitrary code on the target system. Google stated that an exploit for CVE-2023-6345 exists in the wild.

AFFECTED PRODUCTS

- Google Chrome versions before 119.0.6045.199 for Mac and Linux
- Google Chrome versions before 119.0.6045.199/.200 for Windows
- Google Chrome versions before 119.0.6045.193 for Android

REFERENCES

- Google Chrome emergency update fixes 6th zero-day exploited in 2023

SECURITY ADVISORY

Date: Nov 23, 2023

Vulnerabilities in fingerprint sensors can enable hackers to bypass Windows Hello authentication.

RECOMMENDATIONS

1. For the fingerprint reader exploits to take effect, it is crucial that users of the specified laptops have already activated fingerprint authentication. It is recommended to disable Windows Hello fingerprint authentication till the patches are released to fix this issue.

2. Ensure that the device used for fingerprint authentication meets security standards and has not been compromised. Keep the operating system, drivers, and security software up to date.

3. When enrolling fingerprints, do so in a secure environment to prevent unauthorized access during the setup process. Avoid enrolling fingerprints on public computers or devices.

4. Use BitLocker encryption to protect the data on your device. This adds an additional layer of security and helps safeguard sensitive information in case the device is lost or stolen.

5. Ensure that the biometric sensor (fingerprint reader) is physically secure and tamper resistant. This prevents attackers from manipulating the hardware to gain unauthorized access.

6. Consider enabling multi-factor authentication (MFA) along with fingerprint authentication for an extra layer of security. This could include using a PIN or another authentication method.

7. Provide users with information on best practices for using Windows Hello fingerprint authentication and raise awareness about potential security risks.

INTRODUCTION

Researchers at Blackwing Intelligence have identified multiple vulnerabilities affecting fingerprint sensors in Dell Inspiron 15, Lenovo ThinkPad T14, and Microsoft Surface Pro X laptops.

These flaws, present in Goodix, Synaptics, and ELAN sensors, could potentially allow attackers to bypass Windows Hello authentication. Despite the "match on chip" (MoC) security feature, which prevents replaying stored fingerprint data, the researchers uncovered novel attack methods, such as sensor spoofing and cleartext transmission of security identifiers.

On Dell and Lenovo devices, the researchers leveraged a custom Linux-powered Raspberry Pi 4 device to achieve authentication bypass by enrolling an attacker's fingerprint with the valid ID of a legitimate Windows user. The Synaptics sensor, utilizing a custom TLS stack instead of SDCP, was susceptible to this attack.

Additionally, the ELAN sensor on the Surface device lacked SDCP protection, used cleartext USB communication, and had no authentication, allowing researchers to spoof the fingerprint sensor and send valid login responses.

Users are advised to remain vigilant. These vulnerabilities highlight the importance of OEMs enabling Secure Device Connection Protocol (SDCP) and conducting thorough security audits on fingerprint sensor implementations to safeguard against potential exploits.

REFERENCES

- New Flaws in Fingerprint Sensors Let Attackers Bypass Windows Hello Login
- Windows Hello auth bypassed on Microsoft, Dell, Lenovo laptops
- A TOUCH OF PWN - PART I

SECURITY ADVISORY

Date: Nov 08, 2023

The Intricate Puzzle of the LinkedIn Database 2023: Fact or Fiction?

RECOMMENDATIONS

1. Prioritize remediating known exploited vulnerabilities.

2. Ensure that sensitive data is encrypted, both in transit and at rest. This protects it from being accessed or intercepted by unauthorized individuals.

3. Enable MFA for all your online accounts, especially for critical platforms like LinkedIn.

4. Regularly update your passwords and use strong, unique passwords for each online account. Consider using a reputable password manager to help generate and store complex passwords.

5. Review and adjust the privacy settings on your LinkedIn and other social media accounts. Limit the amount of personal information visible to the public and be cautious about sharing sensitive data.

6. Be vigilant about phishing attempts. Attackers may use the data from such breaches to craft convincing phishing emails. Verify the authenticity of emails and avoid clicking on suspicious links or downloading attachments.

7. Regularly monitor your online accounts for unusual activities. Set up alerts or notifications for any unauthorized access or changes to your account.

8. Be aware of data protection regulations and legal obligations that apply to your organization. Ensure compliance with these regulations when handling personal data.

9. Maintain regular backups of your critical data. In the event of a breach, having backup copies of your data can help minimize the impact.

10.Whenever possible, minimize the amount of personal information you share online. Only provide necessary information on social media and other websites.

INTRODUCTION

On November 04, a user named USDoD on Breach Forums released the "LinkedIn Database 2023 2.5 Millions" dataset. The data wasn't being sold but instead made available for free download.

The dataset claimed to contain LinkedIn data from 2023, which, on the surface, seemed plausible given previous breaches and data scrapes. LinkedIn had already suffered significant data breaches in the past, so this new claim appeared credible.

Later, the data was found to be both scraped public data and email addresses constructed from individuals' names. The threat actor claimed the database contains emails, profile data, phones, full names, and more confidential info.

Analysis of the dataset from TroyHunt revealed that it included a staggering number of rows, with many records spanning multiple lines due to line breaks. Within this vast trove, there was a pattern in the way email addresses were formed, using "[first name].[last name]@" as the format. This pattern extended across multiple email addresses linked to the same individual, often resulting in a significant expansion of the total number of email addresses. Further, these email addresses were found to be fabricated. They were constructed by taking the actual domain of the company where the individual worked and then generating the alias from their name. This was done meticulously, with the domains accurately matching the companies the individuals were associated with on their LinkedIn profiles.

Also, on October 31, an archive containing data reportedly scraped from 500 million LinkedIn profiles surfaced on a well-known hacker forum. To prove the authenticity of the breach, the post author leaked 2 million records as a sample. The leaked files contain extensive information about the affected LinkedIn users, including their full names, email addresses, phone numbers, workplace details, and more.

REFERENCES

1. Alleged LinkedIn Data Breach of 816M B2B Profiles Sends Shockwaves
2. Hackers, Scrapers & Fakers: What's Really Inside the Latest LinkedIn Dataset
3. Scraped data of 500 million LinkedIn users being sold online, 2 million records leaked as proof

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

6th Nov 2023 – 19th Nov 2023
TRAC-ID: NII23.11.0.2

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	USN-6462-2: Linux kernel (IoT) vulnerabilities	• Ubuntu 20.04 LTS	Kindly update to fixed version
Ubuntu Linux	USN-6465-3: Linux kernel (GKE) vulnerabilities	• Ubuntu 22.04 LTS	Kindly update to fixed version

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Red Hat Enterprise Linux	RHSA-2023:7294	• Red Hat Enterprise Linux Server - AUS 7.6 x86_64	Kindly update to fixed version
Red Hat Enterprise Linux	RHSA-2023:7265	• Red Hat Enterprise Linux for x86_64 8 x86_64	Kindly update to fixed version

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

6th Nov 2023 – 19th Nov 2023
TRAC-ID: NII23.11.0.2

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2023-6748	• Oracle Linux 9 (aarch64) • Oracle Linux 9 (x86_64)	**Kindly update to fixed version**
Oracle Linux	ELSA-2023-7277	• Oracle Linux 9 (aarch64) • Oracle Linux 9 (x86_64)	**Kindly update to fixed version**

IVANTI

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ivanti Secure Access Client	**Security fixes included in the latest Ivanti Secure Access Client Release**	• All versions of the Ivanti Secure Access Client below 22.6R1.1	**Kindly update to fixed version**

SECURITY ADVISORY