Denis Marincas (20099160)

[Email address]

Security breaches based on software vulnerabilities

The two security breaches I chose to draw a report on are:

* The Colonial Pipeline Attack
* LastPass security incident

To rank these two incidents by I have the The Common Vulnerability Scoring System (CVSS). *CVSS provides a numerical (0-10) representation of the severity of an information security vulnerability. CVSS scores are commonly used by infosec teams as part of a vulnerability management program to provide a point of comparison between vulnerabilities, and to prioritize remediation of vulnerabilities.* (Balbix, 2023)

Website

Description automatically generated with medium confidence

For the ***base metrics*** of these two attacks, three subscore elements are taken into consideration: exploitability, scope and impact.

**Exploitability**

Attack Vector – score is higher if the attack can be carried out from a remote location (i.e outside of a company’s network) compared to a physical attack which requires connection to a physical port.

Attack Complexity – higher score if the attack carried out requires additional work on the attackers side such as decryption or theft of a shared secret key

Privileges required – score is higher if the attacker requires administrative or escalated privileges in order to conduct the attack

User privilege – score is affected by the need of the attacker to interact with external personas in order to accomplish his tasks, whether these are willing or unwitting to participate in this activity. Involvement of multiple external personas increases this score.

**Scope –** scope relates to whether a vulnerability in one component can propagate to other components. The scope is greater if exploiting one vulnerability offers access to other system components/features.

**Impact**

Confidentiality – score varies on the amount of data the attacker gains access to.

Integrity – score varies on the ability of the attacker to modify data that he gained access to.

Availability – score varies on the loss of availability of the exploited system, the longer the system is taken down, the higher the score.

For the ***temporal metrics*** of these two attacks, three subscore elements are taken into consideration: Exploit Code Maturity, Remediation Level, and Report Confidence.

Exploit Code Maturity – score increases over time as the code to exploit a vulnerability matures, becoming more stable and more widely available.

Remediation Level – as patches and fixes for an exploit become available this score lowers

Report Confidence - confidence measures the level of validation demonstrating that a vulnerability is both real and exploitable.

For the ***environmental metrics*** of these two attacks, two subscore elements are taken into consideration: Security Requirements and modifications of Base Metrics.

Security Requirements - *Security Requirements characterize the criticality of the asset in question. Mission critical data or assets get a higher score than less important assets. For example, a vulnerability identified in a database of all customer data would get a higher score than a vulnerability identified in a non-privileged user’s workstation.* (Balbix, 2023)

Modified Base Metrics - *An organization may choose to modify values of the Base CVSS Metrics based on mitigations that they have put into place. For example, “air gapping” a server, or removing any external network connections, will prohibit an attacker from being able to exploit a vulnerability that might otherwise be accessible remotely. The result is that the Attack Vector Base Metric is reduced in this instance.* (Balbix, 2023)

Table

Description automatically generated

LastPass Attack



LastPass is a password manager service. It is used by individuals and big companies such as Google, Amazon etc. to store encrypted passwords online. LastPass has had multiple hackers and groups overtime attempt to obtain their data. Due to the nature of the data and the sensitivity of it, these attacks occurred fairly often but never affecting the user, up until recently.

August 2022 LastPass CEO put out a statement telling LastPass users about an attack on its systems, but said there is nothing to worry about as no customer data had been affected. In a December 22nd update, LastPass puts out one more statement explaining that the initial attack in August saw *“some source code and technical information were stolen from our development environment and used to target another employee, obtaining credentials and keys which were used to access and decrypt some storage volumes within the cloud-based storage service.*” (Sharwood, 2022).

In the latest update it appears that access was gained to their cloud hosted enterprise backups, through credential / keys gained from a hack of LastPass’s development environment, prior to (2022–08–25), through a compromised Developer sign-on: “some source code and technical information were stolen from our development environment and used to target another employee, obtaining credentials and keys which were used to access and decrypt some storage volumes within the cloud-based storage service.” (Toubba, 2022).

Once the attacker gained access, he was able to retrieve information and metadata including company names, email addresses, phone numbers, customer IP addresses, billing addresses and end-user names. Besides this lot of information, “customer vault” data was also copied. This “vault” contains LastPass user passwords. This means the attackers have access to users’ passwords. Fortunately, LastPass uses “256-bit AES encryption and can only be decrypted with a unique encryption key derived from each user’s master password”. (Toubba, 2022) To decrypt the data, the hacker would need the vault’s master password, something only the customer should know.

The problem is that, with all the other information held by the attacker, it wouldn’t be impossible to crack users’ master passwords. Brute-force attacks could be a possibility but as a security measure LastPass requires a master password at least 12 characters long. Users are often extremely lax at choosing good passwords, also two thirds re-use passwords. One of the most plausible ways for the culprit to target inviduals and obtain their master password is by making use of the information he obtained from the customer vault such as their phone number, IP address or email address.

In conclusion, this attack could have been prevented/mitigated if better protection/authentication policies were put in place such as multiple factor authentication when accesing extremely sensitive data such as storage volumes in the cloud.

**LastPass CVSS Scoring:**

Attack Vector – 1/1

Attack Complexity – 1/1

Privileges required – 0.8/1

User privilege – 0.5/1

Confidentiality – 1/1

Integrity – 0.5/1

Availability - 0/1

Exploit code maturity – 0.5/1

Remediation level – 0.9/1

Report confidence – 1/1

**Total : 7.2/10 (high)**

**The Colonial Pipeline Attack**

The Colonial Pipeline attack was carried out by a hacking group called DarkSide. They specialise in ransomware attacks and sell ransomware-as-a-service (RaaS) attacks.

“Ransomware is designed to encrypt the victim's files to extort and ransom for their recovery. DarkSide is a ransomware-as-a-service (RaaS)--the developers of the ransomware received a share of the proceeds from the cybercriminal actors who deploy it, known as "affiliates." This DarkSide ransomware variant executes a dynamic-link library (DLL) program used to delete Volume Shadow copies available on the system. The malware collects, encrypts, and send system information to the threat actor's command and control (C2) domains and generates a ransom note to the victim.” (CISA, 2021) (a link to the full analysis of the ransomware program is available in the references section).

This is what happened to the Colonial Pipeline Company on May 7,2021. It all started from a breached employee personal password. Culprits encrypted all their data and systems so they rendered them unusable on their side. To regain access, Colonial Pipeline paid the amount that was asked by the hacker group (75 bitcoin or 4.4$ million) within several hours. Darkside kept their end of the bargain and released their decryption tool. “On June 7, the Department of Justice announced that it had recovered 63.7 of the bitcoins (approximately $2.3 million) from the ransom payment.” (Wikipedia, 2023)

This attack led to fuel shortages at gas stations, panic buying and chaos amongst the population. People started hoarding gasoline in whatever containers they could get ahold of, airports were shut down temporarily and airline companies had to redeschule many of their flights. DarkSide group apologized for all the inconviniences they caused and said that was not their goal, only to target high-profile companies which can afford to pay big sums.

This attacked could have been prevented if better care was taken when storing and encrypting sensitive data and better authentication procedures would have been in place.

**LastPass CVSS Scoring:**

Attack Vector – 1/1

Attack Complexity – 0.4/1

Privileges required – 0.4/1

User privilege – 0.3/1

Confidentiality – 1/1

Integrity – 0.6/1

Availability - 1/1

Exploit code maturity – 0.2/1

Remediation level – 0.6/1

Report confidence – 0.7/1

**Total : 6.2/10 (medium)**

# References

Ali, F. (2021, June 28). *DarkSide Ransomware: Who Was Behind the Colonial Pipeline Attack?* Retrieved from MakeUseOf: https://www.makeuseof.com/darkside-ransomware-who-was-behind-the-colonial-pipeline-attack/

Balbix. (2023, February Wednesday). *What are CVSS Scores*. Retrieved from Balbix: https://www.balbix.com/insights/understanding-cvss-scores/

CISA. (2021, July 08). *Malware Analysis Report (AR21-189A).* Retrieved from Cybersecurity & Infrastructure Security Agency: https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-189a

Sharwood, S. (2022, December 23). *LastPass admits attackers have a copy of customers’ password vaults.* Retrieved from The Register: https://www.theregister.com/2022/12/23/lastpass\_attack\_update/#:~:text=In%20a%20December%2022nd%20update%20to%20its%20advice,some%20storage%20volumes%20within%20the%20cloud-based%20storage%20service.%E2%80%9D

Toubba, K. (2022, December 22). *Notice of Recent Security Incident.* Retrieved from LastPass: https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/

Wikipedia. (2023, February 5). *Colonial Pipeline ransomware attack.* Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Colonial\_Pipeline\_ransomware\_attack#:~:text=On%20May%207%2C%202021%2C%20Colonial%20Pipeline%2C%20an%20American,cyberattack%20that%20impacted%20computerized%20equipment%20managing%20the%20pipeline.