Security news:

* [**https://thehackernews.com/**](https://thehackernews.com/)
* [**https://www.bitsight.com/blog/best-cybersecurity-news-outlets**](https://www.bitsight.com/blog/best-cybersecurity-news-outlets)
* [**https://portswigger.net/daily-swig/us**](https://portswigger.net/daily-swig/us)
* [**https://journalists.feedspot.com/cyber\_security\_news\_websites/**](https://journalists.feedspot.com/cyber_security_news_websites/)

This is my open source list for CSIR/SOC:

News:

<https://www.darkreading.com/>

<https://www.bleepingcomputer.com/>

<https://news.ycombinator.com/>

<https://nakedsecurity.sophos.com/>

<https://threatpost.com/>

<https://blog.erratasec.com/>

<https://krebsonsecurity.com/>

<https://medium.com/mitre-attack>

Also, worth looking at pastebin and equivalents.

Weekly/Daily Podcasts:

<http://defensivesecurity.org/>

<https://securityledger.com/>

<https://securityweekly.com/>

* If you like Defensive Sec I highly recommend Risky Biz
* https://risky.biz
* Also worth checking out...
* <https://aboutdfir.com/podcasts/>
* [**https://www.hacklido.com/**](https://www.hacklido.com/)
* **-edit: Also for infosec peeps Internet Storm Center Daily is pretty great; https://isc.sans.edu/podcast.html**
* **Jenkins Patches High-Severity Vulnerabilities in Multiple Plugins**

**CVE-2023-40336**

<https://nvd.nist.gov/vuln/detail/CVE-2023-40336#VulnChangeHistorySection>

<https://access.redhat.com/security/cve/cve-2023-40336>

<https://www.securityweek.com/jenkins-patches-high-severity-vulnerabilities-in-multiple-plugins/>

**Jenkins Patches High-Severity Vulnerabilities in Multiple Plugins**  
**CVE-2023-40336**  
**What is CVSS?**   
            CVSS stands for the Common Vulnerability Scoring System. It's a way to evaluate and rank reported vulnerabilities in a standardized and repeatable way. The goal of CVSS is to help you compare vulnerabilities in different applications – and from different vendors - in a standardized, repeatable, vendor agnostic approach.

CVSS generates a score from 0 to 10 based on the severity of the vulnerability. A score of 0 means the vulnerability is less significant than the highest vulnerability with a score of 10, if you're only using CVSS. By using CVSS to prioritize vulnerabilities, you can focus on the most critical ones first and reduce the overall risk to your organization

|  |  |
| --- | --- |
| **CVSS Base Score** | **CVSS Severity Level** |
| 0 | None |
| 0.1 -  3.9 | Low |
| 4.0 -  6.9 | Medium |
| 7.0  -  8.9 | High |
| 9.0  -  10.0 | Critical |

**What is a CVE?**  
          CVE stands for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws.

First launched in 1999, CVE is managed and maintained by the National Cybersecurity FFRDC (Federally Funded Research and Development Center), operated by the MITRE Corporation. CVE entries are brief. They don’t include technical data, or information about risks, impacts, and fixes. Those details appear in other databases, including the U.S. National Vulnerability Database (NVD), the CERT/CC Vulnerability Notes Database, and various lists maintained by vendors and other organizations. Across these different systems, CVE IDs give users a reliable way to recognize unique vulnerabilities and coordinate the development of security tools and solutions. When someone refers to a CVE, they mean a security flaw   
that's been assigned a CVE ID number.

**CVE Identifiers**  
           When vulnerabilities are verified, a CVE Numbering Authority (CNA) assigns a number. A CVE identifier follows the format of — CVE-{year}-{ID}. There are currently 114 organizations, across 22 countries that are certified as CNAs. These organizations include research organizations, and security and IT vendors. CNAs are granted their authority by MITRE, which can also assign CVE numbers directly. Once a vulnerability is reported, the CNA assigns it a number from the block of unique CVE identifiers it holds.

           The CNA then reports the vulnerability with the assigned number to MITRE. Frequently, reported vulnerabilities have a waiting period before being made public by MITRE. This allows vendors to develop patches and reduces the chance that flaws are exploited once known. When a CVE vulnerability is made public, it is listed with its ID, a brief description of the issue, and any references containing additional information or reports. As new references or findings arise, this information is added to the entry.

link: [What is Common Vulnerabilities & Exposures (CVE)](https://www.youtube.com/watch?v=qfpnJyTl1To)

**Jenkins:**  
          Jenkins is a fork of a project called Hudson, which was trademarked by Oracle. Hudson was eventually donated to the Eclipse Foundation and is no longer under development. Jenkins development is now managed as an open source project under the governance of the CD Foundation, an organization within the Linux Foundation.

**In short:**   
Jenkins is an open source continuous integration/continuous delivery and deployment (CI/CD) automation software DevOps tool written in the Java programming language. It is used to implementCI/CD workflows, called pipelines.

**CVE-2023-40336:**  
A flaw was found in the Jenkins Folders Plugin. The  affected versions of this plugin hasallow attackers to copy folders.

link:An introduction to Jenkins for IT operations teams

Reference:   
<https://www.balbix.com/insights/what-is-a-cve/>  
<https://nvd.nist.gov/vuln/detail/CVE-2023-40336#VulnChangeHistorySection>   
<https://www.infoworld.com/article/3239666/what-is-jenkins-the-ci-server-explained.html>  
[https://access.redhat.com/security/cve/cve-2023-40336](https://access.redhat.com/security/cve/cve-2023-40336 )  
[https://www.securityweek.com/jenkins-patches-high-severity-vulnerabilities-in-multiple-plugins/](https://www.securityweek.com/jenkins-patches-high-severity-vulnerabilities-in-multiple-plugins/ )  
<https://www.openwall.com/lists/oss-security/2023/08/16/3>

**Questions need to be Answered:**

1. What is CVSS?

2. What is CVE?

3. Provide  two real-world vulnerability with its corresponding CVSS score and severity level which are dicovered after Jan 2023 and Explain what you understood about the vulnerability

4. What is Jenkins?

5. Explain CVE-2023-40336?

Extra Questions ?

6.Explain the concept of "zero-day vulnerabilities" and the challenges they pose to cybersecurity

7. In the context of Jenkins or similar CI/CD tools, what are some best practices for ensuring the security of automation pipelines?

8. Do one Peer response.

**Data Breach – sample 1**

# Discussion Topic: Understanding the Dynamics of Recent Large-Scale Data Breaches: Case Study on Nelnet and Other Security Incidents

Introduction

In recent months, we have witnessed a surge in data breaches affecting millions of individuals. Notably, the Nelnet Servicing breach affected over 2.5 million student loan borrowers, compromising personal information such as names, addresses, and Social Security numbers. This incident, coupled with other recent breaches, raises serious concerns about the security measures in place to protect user data. This discussion seeks to delve deeper into these incidents, analyze their implications, and foster a conversation on how to mitigate such breaches in the future.

Statistics

1. Nelnet Servicing Breach (Articles 1, 2, and 3):

- Affected Individuals: Over 2.5 million

- Data Compromised: Names, addresses, emails, phone numbers, Social Security numbers

- Period: June 2022 to July 2022

- Discovery: August 2022

- Financial Information: Not compromised

2. Other Recent Breaches (Article 4):

- Topgolf Callaway: Over 1 million customers affected

- Freecycle: 7 million users affected

- Forever 21: 500,000 customers affected

- Duolingo: 2.6 million users affected

- Discord.io: 760,000 users affected

- IBM MOVEit: 4.1 million patients affected

Discussion Points

1. Vulnerability Assessment and Management

- What vulnerability might have been exploited in the Nelnet Servicing breach?

- How can organizations proactively identify and mitigate vulnerabilities before they are exploited?

2. Cybersecurity Training and Awareness

- How can organizations foster a culture of cybersecurity awareness among their employees?

- What role does continuous training and skill development play in preventing data breaches?

3. Legal and Ethical Considerations

- What legal ramifications do companies face in the wake of data breaches?

- How should companies ethically respond to data breaches to minimize harm to affected individuals?

4. Future Implications

- How might the compromised data be used in future social engineering and phishing campaigns?

- Considering the recent student loan forgiveness news, how can individuals protect themselves from potential scams?

5. Technological Solutions

- How can technologies such as multifactor authentication, single sign-on, and adaptive access help in preventing data breaches?

- What role does AI and machine learning play in enhancing security measures?

Questions for Further Discussion

1. How do recent data breaches, like the one at Nelnet, reflect on the current state of cybersecurity in various sectors?

2. How can organizations collaborate to create a more secure cyber environment, especially in sectors holding sensitive data such as financial and healthcare sectors?

3. In light of the recent breaches, what policy changes are necessary at the organizational and governmental levels to enhance data protection?

4. Considering the potential for increased phishing attempts following the breach, how can individuals be educated to identify and avoid such scams?

5. How can organizations develop and maintain a robust incident response plan to handle data breaches more effectively?

We encourage you to bring in case studies, real-life experiences, and insights into this discussion to foster a rich and informative conversation. Let's work together to understand the dynamics of these breaches and brainstorm strategies to prevent such incidents in the future.

Sample 2:

Introduction

In the digital era, the safeguarding of sensitive information is paramount. A data breach occurs when there is an unauthorized access, disclosure, or retrieval of protected and sensitive data. Such breaches can occur through various means including hacking, social engineering, insider threats, or through accidental exposure. The impact of these breaches can be vast, affecting individuals and organizations both financially and reputation. Understanding how a data breach occurs is crucial in devising strategies to prevent them. Typically, a data breach takes place in stages such as identification of vulnerability, infiltration of the network, data access, and finally data extraction.

In recent months, we have witnessed a surge in data breaches affecting millions of individuals. Notably, the Nelnet Servicing breach affected over 2.5 million student loan borrowers, compromising personal information such as names, addresses, and Social Security numbers. This incident, coupled with other recent breaches, raises serious concerns about the security measures in place to protect user data. This discussion seeks to delve deeper into these incidents, analyze their implications, and foster a conversation on how to mitigate such breaches in the future.

Statistics

1. Nelnet Servicing Breach (Articles 1, 2, and 3):

- Affected Individuals: Over 2.5 million

- Data Compromised: Names, addresses, emails, phone numbers, Social Security numbers

- Period: June 2022 to July 2022

- Discovery: August 2022

- Financial Information: Not compromised

2. Other Recent Breaches (Article 4):

- Topgolf Callaway:

- Affected Individuals: Over 1 million customers

- Data Compromised: Full names, shipping addresses, email addresses, phone numbers, account passwords, and security question answers

- Notification: September 2023

- Freecycle:

- Affected Individuals: 7 million users

- Data Compromised: User IDs and email addresses

- Notification: September 2023

- Forever 21:

- Affected Individuals: 500,000 customers

- Data Compromised: Names, dates of birth, bank account information, and Social Security numbers

- Notification: August 2023

- Duolingo:

- Affected Individuals: 2.6 million users

- Data Compromised: Names, email addresses, phone numbers, social media information, and languages studied at the time of the breach

- Notification: August 2023

- Discord.io:

- Affected Individuals: 760,000 users

- Data Compromised: Passwords, usernames, Discord IDs, and billing addresses

- Notification: August 2023

- IBM MOVEit:

- Affected Individuals: 4.1 million patients

- Data Compromised: Sensitive healthcare data

- Notification: August 2023

Mitigating Data Breaches

Mitigating data breaches requires a proactive and multi-faceted approach. Here are some strategies and tools that can be employed:

1. Regular Vulnerability Assessments and Penetration Testing (VAPT): Conduct regular VAPT to identify and patch vulnerabilities before they can be exploited.

2. Employee Training and Awareness: Develop training programs to educate employees about the potential risks and how to avoid falling prey to phishing and social engineering attacks.

3. Implementation of Multi-Factor Authentication (MFA): Utilize MFA to add an extra layer of security, making it harder for attackers to gain unauthorized access.

4. Data Encryption: Employ data encryption to protect data both at rest and in transit, ensuring that even if data is accessed, it cannot be read without the necessary decryption keys.

5. Incident Response Plan: Develop a robust incident response plan to quickly contain and remediate breaches when they occur.

6. Utilizing Security Tools:

- Firewalls: To block unauthorized access to or from a private network.

- Antivirus Software: To protect against malware and other cyber threats.

- Security Information and Event Management (SIEM): To provide real-time analysis of security alerts generated by applications and network hardware.

7. Legal Compliance and Regulations: Ensure compliance with legal and regulatory requirements concerning data protection and privacy.

Discussion Points

From sample 1:  
  
  
Scenario 1:

### Scenario

Imagine that you are an intern at a rapidly growing startup called "HealthPulse", which specializes in wearable health monitors. One morning, the company discovers that there has been a data breach where sensitive customer data, including health metrics and personal information, has been accessed by unauthorized individuals. As part of your internship, you are asked to assist in managing the aftermath of this data breach. Your task is to draft an initial response plan outlining the steps the company should take immediately following the discovery of the breach.

### Key Points to Address in the Answer

1. \*\*Incident Identification and Confirmation\*\*

- Confirming the data breach has occurred through logs and unusual activity patterns.

- Identifying the nature of data that has been breached.

2. \*\*Communication and Notification\*\*

- Informing the company's leadership team about the breach.

- Preparing a communication plan to notify affected customers transparently and timely, in compliance with legal requirements.

3. \*\*Involvement of Cybersecurity Experts\*\*

- Engaging a team of cybersecurity experts to investigate the breach and to prevent further data loss.

- Collaborating with IT teams to secure the compromised systems.

4. \*\*Legal and Regulatory Compliance\*\*

- Consulting with the legal team to understand the implications of the breach and the company’s responsibilities.

- Reporting the breach to relevant government and regulatory bodies, if necessary.

5. \*\*Public Relations and Media Handling\*\*

- Developing a media handling strategy to manage potential reputational damage.

- Preparing press releases and official statements to keep the public informed about the steps the company is taking to resolve the issue.

6. \*\*Remedial Actions and Future Prevention Strategies\*\*

- Developing a remedial action plan to address the vulnerabilities that led to the breach.

- Initiating a review of current security policies and implementing stronger measures to prevent future breaches.

7. \*\*Customer Support and Assistance\*\*

- Setting up a helpline and support system to assist affected customers.

- Offering credit monitoring services or other assistance to affected customers to mitigate the potential consequences of the breach.

8. \*\*Learning and Improvement\*\*

- Conducting a post-incident review to learn from the breach and to improve the company's data security protocols.

- Implementing educational programs for employees to foster a culture of data security and privacy.

### Sample Answer

In light of the recent data breach at HealthPulse, it is imperative that we act swiftly and responsibly to mitigate the consequences of this incident. First and foremost, we need to confirm the extent of the breach by reviewing system logs and identifying the compromised data. Concurrently, a team of cybersecurity experts should be engaged to investigate the breach further and secure the compromised systems to prevent further data loss.

As a responsible organization, we must transparently communicate the incident to affected customers, keeping them informed about the steps we are taking to resolve the issue. This should be coordinated with the public relations team to manage potential reputational damage and to keep the public informed through press releases and official statements.

Legally, we must consult with our legal team to understand the implications of the breach and to ensure compliance with necessary regulations, including reporting the breach to relevant government and regulatory bodies.

To prevent future occurrences, a comprehensive remedial action plan should be developed to address the vulnerabilities that led to the breach. This includes reviewing and strengthening our current security policies and implementing advanced security measures such as data encryption and multi-factor authentication. Moreover, we should offer support to affected customers, possibly including credit monitoring services, to mitigate the potential adverse effects of the breach.

Lastly, this incident serves as a learning opportunity for us. A post-incident review should be conducted to identify the lessons learned and to foster a culture of data security and privacy within the organization through educational programs for employees.

By adopting this comprehensive approach, we aim to navigate this challenging situation responsibly and to regain the trust of our customers and stakeholders.

Scenario 2:

### Scenario

You are a data security analyst at Freecycle, a non-profit organization facilitating the exchange of used items to prevent them from ending up in landfills. On August 30, the organization discovered a significant data breach, jeopardizing the personal information of over 7 million users. It transpired that the breach had occurred several months prior, with the data being available for sale on the dark web since at least June. The compromised data includes usernames, User IDs, email addresses, and MD5-hashed passwords.

Regrettably, the credentials of Freecycle's founder and executive director, Deron Beal, were among the stolen data, providing the threat actors with extensive access to the organization's member information and forum posts. The incident has raised concerns about potential phishing attacks and identity thefts that could follow.

Your role is pivotal in developing a robust strategy to not only manage the current crisis but also to prevent such incidents in the future. You are tasked to create an action plan that addresses the immediate concerns and outlines long-term strategies to enhance data security. This plan will be presented to the board of directors and the general membership to restore faith in the organization's ability to safeguard user data.

### Key Points to Address in the Answer

1. \*\*Immediate Containment and Investigation\*\*

- Identifying and securing the vulnerabilities that led to the breach.

- Collaborating with cybersecurity experts to investigate the nature and extent of the breach.

2. \*\*User Notification and Assistance\*\*

- Formulating a clear and transparent communication strategy to notify affected users.

- Guiding users on how to reset their passwords and advising them to change passwords on other platforms if the same credentials were used.

3. \*\*Legal Compliance and Cooperation with Authorities\*\*

- Reporting the breach to relevant regulatory bodies in the US and the UK, including the Information Commissioner’s Office (ICO).

- Collaborating with law enforcement agencies in the investigation process.

4. \*\*Public Communication and Reputation Management\*\*

- Crafting public statements and press releases to keep the public informed and to manage potential reputational damage.

- Utilizing social media and other platforms to disseminate information and updates regarding the breach.

5. \*\*Long-term Security Enhancement\*\*

- Conducting a comprehensive review of the existing security infrastructure.

- Developing and implementing a multi-faceted security strategy that includes advanced security measures like multi-factor authentication and data encryption.

6. \*\*Education and Training\*\*

- Initiating a training program to educate employees on data security best practices and fostering a culture of vigilance within the organization.

- Developing resources to educate users on how to protect themselves from phishing attempts and identity thefts.

7. \*\*Future Preparedness\*\*

- Creating a robust incident response plan to ensure a coordinated and effective response to potential future data breaches.

- Regularly updating the organization's data security policies to adapt to evolving cyber threats.

### Sample Answer

In the wake of the recent data breach at Freecycle, we are committed to taking decisive actions to manage the crisis effectively and to prevent such incidents in the future. Our immediate focus is on containing the breach by identifying and securing the vulnerabilities that were exploited. We have engaged a team of cybersecurity experts to conduct a thorough investigation into the breach to understand its nature and extent.

As part of our commitment to transparency, we are developing a communication strategy to notify affected users about the breach. We will guide them on how to reset their passwords and advise them to change passwords on other platforms where the same credentials might have been used. We are also setting up a dedicated support line to assist users during this period.

In compliance with legal requirements, we have reported the breach to the relevant regulatory bodies in the US and the UK, including the Information Commissioner’s Office (ICO). We are cooperating fully with law enforcement agencies in their investigation.

To manage the potential reputational impact of this breach, we are crafting public statements and press releases to keep the public informed about the steps we are taking to address the issue. We will leverage social media and other platforms to disseminate information and updates regarding the breach effectively.

Looking forward, we recognize the need to enhance our data security infrastructure. We are conducting a comprehensive review of our existing security protocols and developing a multi-faceted security strategy that includes the implementation of advanced security measures like multi-factor authentication and data encryption.

To foster a culture of vigilance within our organization, we are initiating a training program to educate employees on data security best practices. We will also develop resources to educate users on protecting themselves from phishing attempts and identity thefts.

Lastly, we are developing a robust incident response plan to ensure a coordinated and effective response to potential future data breaches. We pledge to regularly review and update our data security policies to adapt to the rapidly evolving landscape of cyber threats, to safeguard the trust and security of our nearly 11 million members worldwide.