ICRC Data Breach:
An RCE Attack Linked to Iranian Influence Operation

By: Mike Rebultan

Literature Review

In November 2021, hackers gained access to servers hosting the personal data of more than 500,000 people receiving assistance from the International Committee for the Red Cross (ICRC) and the Red Crescent Movement. The breach was discovered in January 2022 when the hackers offered to sell the stolen data online. The email address used by the hackers was later found to have been used to register domains linked to an Iranian media influence operation.

The vulnerability used to gain access was an authentication bypass vulnerability in Zoho ManageEngine ADSelfService Plus. As a result of this vulnerability, attackers are able to execute remote code on the target system, compromising the system and enabling them to access sensitive data.

The ICRC updated its statement about the breach on February 7th, stating that the hackers had used an unpatched critical vulnerability to gain access to the servers. It was possible for the hackers to deploy offensive security tools, disguising themselves as legitimate users or administrators and accessing the encrypted data.

The FBI has linked the email address used by the hackers to a media influence operation originating from Iran. This operation used a network of inauthentic news sites and social media accounts to promote narratives in line with Iranian interests, including anti-Saudi, anti-Israeli, and pro-Palestinian themes.

The incident highlights the need for organizations to prioritize cybersecurity and safeguard they keep their systems updated with patches and updates. The exploitation of an unpatched vulnerability is a common attack vector for hackers to gain access to systems and steal data. In addition, organizations must remain vigilant and be prepared to respond to cyber incidents when they occur to mitigate the damage caused.

While the exact tactics, techniques, and procedures (TTPs) used by the hackers to compromise the ICRC are not known, the exploitation of the vulnerability in Zoho ManageEngine ADSelfService Plus is likely to have been a key component. Once they gained access, the hackers used offensive security tools to disguise themselves as legitimate users or administrators, allowing them to access the encrypted data despite its protection.

It is possible that the hackers used social engineering tactics to trick employees of the ICRC into divulging login credentials or other sensitive information that could have helped them gain access to the servers. The hackers may also have used spear-phishing emails to target individuals within the organization with malware that could allow them to gain a foothold in the network.

Another possibility is that the hackers used a supply chain attack to gain access to the ICRC servers. In this attack, hackers compromise a third-party vendor that has access to the target organization's systems and use that access to launch an attack.

Regardless of the specific TTPs used, the incident highlights the need for organizations to have robust cybersecurity defenses and to safeguard that their employees are trained to detect and respond to suspicious activity. Additionally, organizations must keep their systems updated with the latest security patches and use multi-factor authentication to protect against unauthorized access.

McCumbers Cube

The McCumber Cube is a framework for information security developed by John McCumber in 1991. It is designed to help organizations evaluate their security posture by analyzing three primary security concerns: confidentiality, integrity, and availability.

The cube represents these concerns, with confidentiality, integrity, and availability forming the X, Y, and Z axes, respectively. The framework helps organizations to identify and understand the relationships between the three security concerns and to develop appropriate security strategies based on these relationships. As a result, organizations can use the McCumber Cube to identify potential security gaps and create a more comprehensive and practical approach to information security.

McCumbers Cube Application

Applying the McCumbers Cube to this incident can help identify the security gaps in the ICRC's cybersecurity defenses. The McCumbers Cube is a security model that consists of three dimensions: the policy dimension, the technology dimension, and the people dimension. By examining each of these dimensions, the ICRC can identify areas where its security posture is lacking and take steps to improve its defenses.

In the policy dimension, the ICRC can examine its cybersecurity policies and procedures to determine whether they were effective in preventing and responding to a data breach. This can include reviewing their incident response plan, data retention policies, and access control policies to safeguard they are up-to-date and effective.

In the technology dimension, the ICRC can assess its cybersecurity technology to identify any gaps or weaknesses. This can include reviewing their network security, endpoint security, and data encryption practices to safeguard that they are robust and effective in protecting sensitive data.

In the people dimension, the ICRC can examine its employee training and awareness programs to determine whether they were effective in preventing social engineering attacks and other forms of human error. This can include reviewing their security awareness training, phishing simulations, and other employee education initiatives to safeguard that they are effective in preventing and responding to cybersecurity incidents.

By applying the McCumbers Cube to this incident, the ICRC can gain a better understanding of its security gaps and take steps to improve its cybersecurity defenses. This can help prevent future data breaches and safeguard that sensitive data is protected against cyber threats.

McCumbers Cube Cell				
		Storage	Processing	Transmission
Confidentiality	Policy	1	2	3
	Training	4	5	6
	Technology	7	8	9
Integrity	Policy	10	11	12
	Training	13	14	15
	Technology	16	17	18
Availability	Policy	19	20	21
	Training	22	23	24
	Technology	25	26	27

Findings and Analysis

1. Confidentiality and Storage

The confidentiality and storage aspects are relevant to the ICRC incident as the hackers were able to gain access to servers hosting the personal data of over 500,000 people receiving assistance from the organization. This data was sensitive and included personally identifiable information that should have been kept confidential.

To thwart similar incidents in the future, the ICRC should implement strong access controls and encryption to protect the confidentiality of stored data. This includes limiting access to sensitive data to only those who need it, such as administrators and relevant personnel, and implementing role-based access control to safeguard that users only have access to the information necessary to perform their duties. The organization should also consider implementing data loss prevention solutions that can detect and prevent unauthorized access to sensitive information. Finally, the ICRC should safeguard that all stored data is encrypted – both at rest and in transit to protect against data exfiltration in the event of a breach.

- Security Policy:

Establish a comprehensive data classification policy that categorizes data based on its sensitivity and importance to the organization. This policy should be regularly reviewed and updated to safeguard that it reflects the changing nature of the data that the organization handles.

Develop a clear set of guidelines for the storage and handling of sensitive data. This should include policies around encryption, access controls, and data retention periods.

Implement a formal patch management policy to safeguard that all systems are regularly updated with the latest security patches to prevent the exploitation of vulnerabilities.

- Education or Training:

Conduct regular security awareness training for all employees, emphasizing the importance of data confidentiality and the role that they play in maintaining the security of the organization's data.

Provide specific training to employees who handle sensitive data, including best practices for data storage, transmission, and disposal.

Train employees to detect and report suspicious activity and provide transparent reporting channels.

- Technology:

Implement access controls that limit access to sensitive data to only those who require it to perform their job functions.

Deploy data loss prevention (DLP) technology to monitor and control the movement of sensitive data within the organization and alert on any unauthorized access or data exfiltration attempts.

Use encryption to protect sensitive data at rest and in transit and safeguard that all encryption keys are adequately secured.

By implementing these policies, providing education and training, and using appropriate technology, organizations can reduce the risk of a data breach, and prevent incidents similar to the ICRC from happening again.

2. Confidentiality and Processing

The confidentiality of processing data is relevant to the ICRC incident. The hackers were able to access the encrypted data once they gained access to the servers, suggesting that the encryption algorithm or key may have been compromised.

To prevent such incidents, organizations should safeguard that their data is protected by strong encryption algorithms and keys that are regularly rotated. They should also implement access controls that restrict access to data only to authorized personnel. It is also important to train employees on best practices for data handling and safeguard that they understand the importance of maintaining the confidentiality of sensitive information.

Additionally, organizations should regularly audit their data processing systems to identify any vulnerabilities that may exist and take steps to mitigate them.

- Security Policy:

Implement a data classification policy that categorizes the level of confidentiality for different types of data and sets appropriate access controls for each category.

Develop and enforce a security policy that requires regular audits and vulnerability assessments to identify and mitigate potential security risks.

- Education and Training:

Provide regular cybersecurity awareness training for employees to educate them about the risks of data breaches and the importance of protecting confidential data.

Train employees on the proper use of processing applications, such as Zoho ManageEngine ADSelfService Plus, to safeguard that they are using the applications in a secure manner and are aware of potential vulnerabilities.

- Technology:

Implement encryptions for all sensitive data stored or processed on servers to safeguard that data is protected both in transit and at rest.

Deploy intrusion detection and prevention systems (IDPS) to monitor network traffic and detect suspicious activity that may indicate a breach. This can help to prevent data exfiltration and safeguard that data is kept confidential.

3. Confidentiality and Transmission

Confidentiality and Transmission are relevant to the ICRC incident, as the hackers were able to gain unauthorized access to sensitive data and transmit it out of the organization.

To prevent such incidents, organizations should implement encryption for data in transit to protect it from being intercepted and accessed by unauthorized entities. This can be achieved using secure protocols such as HTTPS or VPNs. Additionally, organizations should restrict access to sensitive data to only authorized personnel and use multi-factor authentication to prevent unauthorized access.

Regular security awareness training for employees can also help to prevent social engineering attacks and safeguard that staffs are aware of the risks associated with sharing sensitive information over email or other communication channels.

- Security Policy:

The organization should develop and enforce strict policies regarding the transmission of sensitive data.

All data transmitted over the network should be encrypted using secure protocols such as TLS.

The organization should also implement strict access controls to safeguard that only authorized users have access to sensitive data during transmission.

- Education and Training:

The organization should provide regular training and awareness sessions to employees to educate them on best practices for secure data transmission.

Employees should be trained on how to recognize and report suspicious emails or messages that may be used to trick them into divulging sensitive information.

- Technology:

The organization should implement secure transmission protocols such as HTTPS, SSH, and VPNs to encrypt data in transit.

The use of secure file transfer protocols such as SFTP and FTPS should also be encouraged.

The organization should also implement intrusion detection and prevention systems to monitor network traffic for suspicious activity and block unauthorized access to sensitive data.

By implementing these recommendations, the organization can safeguard that sensitive data is protected during transmission and moderate the risk of a data breach or unauthorized access.

4. Integrity and Storage

The integrity of data stored in the ICRC's servers was compromised in the incident.

The attackers were able to gain access to the encrypted data by using offensive security tools that allowed them to disguise themselves as legitimate users or administrators. To prevent similar incidents in the future, the ICRC should safeguard that their data is adequately secured by implementing robust encryption protocols, restricting access to sensitive information, and regularly monitoring their systems for suspicious activity. They should also consider using data backup and recovery solutions to mitigate the impact of any future attacks on the integrity of their data.

- Security policy:

Implement data encryption for data-at-rest to prevent unauthorized access to sensitive information.

Conduct regular vulnerability assessments and penetration testing (VAPT) to identify and address potential exposures in the storage infrastructure.

Implement a strong access control policy, limiting access to sensitive data to authorized personnel only.

- Education and training:

Conduct regular security awareness training for employees, including best practices for data storage, password management, and access control.

Train employees on how to identify and report suspicious activity related to data storage and integrity.

- Technology:

Implement intrusion detection and prevention systems to monitor for suspicious activity related to data storage and integrity.

Implement file integrity monitoring (FIM) to detect any unauthorized modifications or deletions of sensitive files.

Use backup and disaster recovery solutions to prevent data loss or exploitation in the event of a breach or other incident.

By implementing these recommendations, organizations can enhance the integrity and security of their stored data, mitigating the risk of incidents like the one experienced by the ICRC.

5. Integrity and Processing

Integrity and processing are relevant to the ICRC incident as the hackers were able to execute remote code on the target system and compromise the system, enabling them to access sensitive data. To prevent similar incidents, organizations should safeguard the integrity of their systems by implementing proper access controls and monitoring user activities.

They should also regularly conduct vulnerability assessments and penetration testing to identify and patch vulnerabilities in their systems. Additionally, organizations should consider implementing file integrity monitoring (FIM) to detect and alert to any unauthorized changes to critical system files and configurations. By ensuring the integrity of their systems, organizations can prevent unauthorized access and manipulation of sensitive data.

- Security policy:

Implement access controls to safeguard that only authorized personnel can access and modify data in processing.

Establish a change management policy that safeguards any changes made to data or software are documented and approved.

- Education or training:

Provide training for employees on the importance of maintaining data integrity and the procedures for handling sensitive data.
Conduct regular awareness programs to inform employees about the latest cyber threats and how to identify and report suspicious activities.

- Technology:

Implement intrusion detection and prevention systems to detect any attempts to modify data in processing.

Use file integrity monitoring tools to track any changes made to data in processing.
Implement encryption for sensitive data at rest and in transit to prevent unauthorized access or modification.

6. Integrity and Transmission

Integrity and Transmission are relevant to the ICRC incident as the hackers were able to gain access to sensitive data and exfiltrate it from the organization's servers. This

highlights the need for organizations to implement strong encryption and other measures to safeguard the integrity of their data in transit. Additionally, it is crucial for organizations to monitor their network traffic and implement intrusion detection and prevention systems to detect and prevent unauthorized access and data exfiltration.

Organizations should also safeguard that their employees are trained to detect and respond to suspicious activity and that they follow best practices for secure communication and data handling.

Finally, it is recommended that organizations conduct regular security audits and vulnerability assessments (VA) to identify and address potential weaknesses in their systems and processes.

- Security Policy:

Implement access control policies to prevent unauthorized access to critical systems and data during transmission.

Enforce encryptions for all sensitive data in transit to prevent interception and modification.

Regularly monitor and audit transmission logs to detect any anomalies or unauthorized access attempts.

Develop an incident response plan to safeguard a quick and effective response in case of any data integrity breaches during transmission.

- Education and Training:

Provide training to employees on secure transmission practices, including the use of encryption and secure communication channels.

Conduct regular security awareness training to safeguard employees are aware of the risks of data tampering during transmission.

Conduct regular phishing simulations to train employees on how to detect and avoid malicious emails that may contain malware or other threats.

- Technology:

Implement encryption technologies to secure sensitive data in transit.

Deploy intrusion detection and prevention systems to monitor network traffic and detect any attempts to compromise data integrity during transmission.

Implement access control mechanisms to restrict access to critical systems and data. Implement multi-factor authentication to prevent unauthorized access to systems and data during transmission.

By implementing these security measures, the risk of data integrity breaches during transmission can be significantly reduced, ensuring that incidents like the ICRC breach do not happen in the future.

7. Availability and Storage

The relevant aspect of the ICRC incident to the combination of Availability and Storage is the impact of the attack on the availability of the stored data. The attackers were able to gain access to the ICRC servers hosting the personal data of more than 500,000 people receiving assistance, and this compromise likely resulted in the unavailability of the data to authorized users.

To mitigate the impact of such an attack, organizations should implement a defense-in-depth strategy, including redundancy and backup systems, to safeguard that data availability is not compromised in the event of a security incident. Regular testing and verification of backups are also recommended to safeguard that they can be restored quickly in the event of an attack.

Additionally, incident response plans should be developed and tested to safeguard that organizations can quickly and effectively respond to a security incident and minimize the impact on data availability.

- Security policy:

Regularly perform backups and store them securely to safeguard that critical data can be recovered in case of a system failure or cyber-attack.

Implement access controls to limit the number of people who can access sensitive data stored in the organization's storage systems.

Safeguard that storage systems are properly configured and hardened to prevent unauthorized access.

- Education or training:

Conduct regular security awareness training for all employees to help them identify potential threats to availability and storage systems.

Teach employees how to properly configure and use storage systems to prevent data loss or corruption.

- Technology:

Use redundancy and failover mechanisms to safeguard that critical data is always available and accessible even in case of a system failure.

Implement intrusion detection and prevention systems to help identify and prevent cyber-attacks that could affect availability and storage systems.

Regularly test and update storage systems to safeguard that they are properly configured and up-to-date with the latest security patches and updates.

8. Availability and Processing

In the context of the ICRC incident, the combination of Availability and Processing is relevant. The hackers were able to execute remote code on the target system, compromising the system and enabling them to access sensitive data. This indicates

a compromise in the availability of the processing system, which could have been prevented if appropriate security measures were in place.

It is important for organizations to safeguard the availability of their processing systems by implementing redundancy, backup, and disaster recovery solutions. In addition, proper access controls, authentication mechanisms, and regular security audits can help prevent unauthorized access and protect the integrity and confidentiality of sensitive data.

- Security Policy:

Implement a comprehensive incident response plan that includes regular backups of critical data and recovery procedures in case of a data breach or loss.
Establish clear guidelines and controls for data access and processing, such as role-based access controls and data encryption protocols, to prevent unauthorized access or tampering.

Conduct regular vulnerability assessments and penetration testing to identify and mitigate potential security risks.

- Education and Training:

Provide regular cybersecurity awareness training for employees to safeguard they are aware of potential threats and how to respond to them.

Train employees to identify and report suspicious activity, including phishing emails or unauthorized access attempts.

- Technology:

Implement network segmentation to separate critical data and systems from other parts of the network, reducing the risk of widespread data loss or compromise in case of a breach.

Deploy intrusion detection and prevention systems to identify and block potential attacks on critical systems.

Use secure communication protocols and robust encryption methods to protect data in transit and safeguard its integrity and availability.

Consider implementing redundant or backup systems to safeguard business continuity in case of a system failure or outage.

9. Availability and Transmission

The relevance of Availability and Transmission to the ICRC incident is significant. The attackers gained access to the ICRC's servers and were able to exfiltrate sensitive data. As a result, there was a breach of availability and transmission of this data to unauthorized individuals.

To prevent similar incidents, organizations should implement measures to safeguard the availability and transmission of their data. This includes having a robust incident response plan in place, performing regular backups, implementing secure

communication protocols, and utilizing network segmentation to limit access to sensitive data. In addition, organizations should provide training to their employees on the importance of safeguarding data and on how to detect and respond to suspicious activity.

- Security Policy:

Develop a comprehensive incident response plan that includes procedures for detecting and responding to DDoS attacks that can impact the availability of transmission resources.

Establish a policy for monitoring network traffic to identify abnormal spikes in traffic patterns that could indicate a DDoS attack.
Develop policies to regulate the use of data transmission resources by employees, contractors, and third-party vendors to safeguard that they do not inadvertently compromise the availability of resources through careless actions.

- Education and Training:

Provide regular training to employees and contractors on how to detect and report suspicious network activity that may indicate a DDoS attack.

Provide training on how to respond to DDoS attacks to minimize their impact on the availability of transmission resources.

Educate employees and contractors on the importance of network security and the potential consequences of compromising the availability of transmission resources.

- Technology:

Deploy advanced network monitoring tools that can detect and mitigate DDoS attacks in real time.

Implement a network architecture that includes multiple layers of security controls, including firewalls, intrusion detection/prevention systems, and load balancers, to help prevent DDoS attacks from succeeding.

Safeguard that critical transmission resources, such as DNS servers and load balancers, are redundant and can withstand the impact of a DDoS attack.

By implementing these recommendations, organizations can improve the availability of transmission resources and prevent similar incidents from happening in the future.

Future Study

To avoid future data breaches and prevent a recurrence of incidents like the one experienced by the International Committee for the Red Cross (ICRC), all organizations, including healthcare and other sectors, should take a comprehensive approach to improve their cybersecurity defenses. A defense-in-depth strategy that incorporates multiple layers of security, such as firewalls, intrusion detection and prevention systems, and antivirus software, can help protect against cyber threats. Additionally, cyber resilience practices, including regular security testing and assessments and the development of a robust incident response plan, can help organizations prepare for, respond to, and recover from cyber-attacks.

In addition to these best practices, organizations should also take proactive steps to improve their cybersecurity defenses. These steps include keeping systems up to date with security patches and updates, using multi-factor authentication, regularly training employees on cybersecurity best practices, monitoring network activity, and reviewing cybersecurity policies and procedures in order to keep them relevant and effective.

Conducting regular risk assessments can also help identify areas of vulnerability and guide actions to address them.

The bottom line, it is essential that organizations, particularly those that handle sensitive data, prioritize cybersecurity and take a comprehensive approach to protect themselves and their clients. By applying defense-in-depth and cyber resilience best practices, in conjunction with these proactive steps, organizations can significantly reduce the risk of cyberattacks and protect sensitive data against cyber threats.

References

- https://krebsonsecurity.com/2022/02/red-cross-hack-linked-to-iranian-influence-operation/#more-58533
- https://securityboulevard.com/2022/02/red-cross-hack-linked-to-iranian-influence-operation/
- https://securityaffairs.com/128110/hacking/nation-state-actors-hacked-red-cross-exploiting-a-zoho-bug.html
- https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know
- https://www.ncyte.net/faculty/cybersecurity-curriculum/college-curriculum/interactive-lessons/the-mccumber-cube-and-cia-triad
- https://nvd.nist.gov/vuln/detail/CVE-2021-40539
- https://cwe.mitre.org/data/definitions/287.html