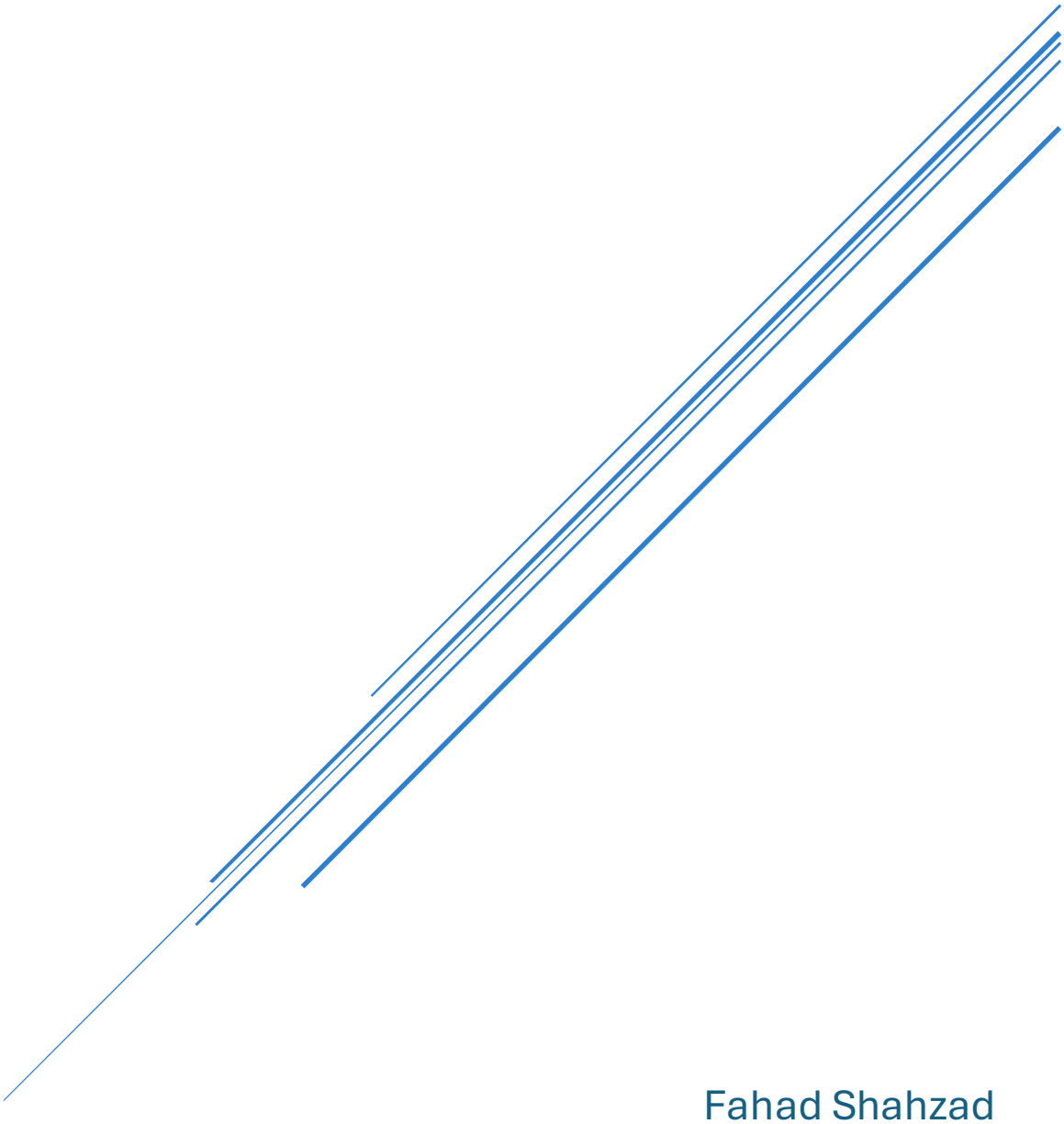
UNITED NATIONS DATA BREACH

Investigation & Research Report



Fahad Shahzad
Project 9

Executive Summary

In August 2019, the United Nations (UN) experienced a significant data breach across multiple offices, including the United Nations Office at Geneva (UNOG), the United Nations Office at Vienna (UNOV), and the Office of the High Commissioner for Human Rights (OHCHR). The breach exploited a critical vulnerability in Microsoft SharePoint (CVE-2019-0604), enabling attackers to infiltrate UN networks and exfiltrate approximately 400 GB of sensitive data. This incident highlighted severe shortcomings in the UN's cybersecurity defenses, necessitating immediate remediation efforts and prompting a reassessment of its security protocols.

Introduction

The UN data breach of 2019 showed the lack of growth in the threat landscape faced by international organizations, where sophisticated cyber-attacks aim to compromise sensitive information for strategic, political, or economic gain. This report provides a detailed analysis of the breach, including the attackers' methods, motivations, the impact of the breach, immediate remediation measures, and recommendations for enhancing cybersecurity resilience.

Methodology

This report employs a structured approach to analyze the United Nations (UN) data breach of 2019, aiming to provide a comprehensive understanding of the incident and its implications for cybersecurity practices within international organizations. The methodology involves gathering and compiling information from multiple sources, including cybersecurity reports, industry analyses, and insights derived from frameworks such as the MITRE ATT&CK.

Analysis

The attackers exploited CVE-2019-0604, a vulnerability in Microsoft SharePoint, to initiate the breach. This vulnerability allowed for remote code execution, enabling unauthorized access to UN networks. Once inside, the attackers employed sophisticated techniques, including lateral movement across the network and automated data exfiltration, evading detection for an extended period.

Victims and Targeted Systems

The breach affected UNOG, UNOV, and OHCHR from July 2019, with unauthorized access detected in August 2019. Attackers targeted SharePoint servers and other internal systems housing sensitive data.

Motivation and Outcome

The attackers tried to obtain sensitive information, including personal data, medical records, and commercial contracts, for intelligence purposes. This breach caused operational disruption and significant reputational damage to the UN.

Technological Analysis:

Exploitation of Vulnerability (T1190: Exploit Public-Facing Application): The attackers exploited a known vulnerability in SharePoint to gain initial access.

Lateral Movement (T1078: Valid Accounts): Once inside, they used legitimate credentials to move laterally across the network, accessing additional systems.

Data Exfiltration (T1020: Automated Exfiltration): Data was exfiltrated using automated techniques to avoid detection.

Recommendations

To mitigate future risks and strengthen cybersecurity posture, the following recommendations are proposed:

Enhanced Patch Management:

- Implement a structured patch management process (NIST SP 800-40) that includes regular assessments
- Prioritization of patches based on risk (NIST SP 800-40 Rev. 3)
- Timely deployment to mitigate vulnerabilities such as CVE-2019-0604.

Advanced Threat Detection:

- Deploy advanced intrusion detection and prevention systems (IDPS) (NIST SP 800-94)

Data Protection Measures:

- Utilize strong encryption protocols (NIST SP 800-57) for sensitive data both at rest and in transit
- Implement access controls (NIST SP 800-53)
- Network segmentation (NIST SP 800-82) to limit unauthorized access and lateral movement within the network.

Comprehensive Incident Response:

- Develop and regularly test a comprehensive incident response plan (NIST SP 800-61 Rev. 2) that outlines roles, responsibilities, and predefined actions for detecting, responding to, and recovering from cybersecurity incidents. Conduct tabletop exercises to simulate breach scenarios and refine response procedures.

Conclusion

The UN data breach of 2019 serves as a stark reminder of the vulnerabilities faced by international organizations in today's digital landscape. The exploitation of a known vulnerability in Microsoft SharePoint led to the unauthorized access and exfiltration of substantial amounts of sensitive data, resulting in operational disruption and reputational harm. Immediate post-breach actions included patching the exploited vulnerability and enhancing network monitoring.

Moving forward, it is imperative for the UN and similar organizations to prioritize cybersecurity resilience through proactive measures such as robust patch management, advanced threat detection, and comprehensive incident response planning. By implementing these recommendations, organizations can mitigate risks, protect sensitive information, and safeguard critical operations against evolving cyber threats.

References

Gatlan, S. (2024, April 19). United Nations agency investigates ransomware attack, data theft. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/united-nations-agency-investigates-ransomware-attack-claimed-by-8Base-gang/#:~:text=UN%20networks%20in%20Geneva%20and,as%20a%20%22major%20meltdown.%22

Cyber Security Hub. (2023, August 29). *Incident of the Week: Leak discloses UN data breach from 2019*. https://www.cshub.com/attacks/articles/incident-of-the-week-leak-discloses-un-2019-breach-from-2019

Staff, D. R. (2023, December 11). *United Nations Data Breach Started with Microsoft SharePoint Bug*. https://www.darkreading.com/threat-intelligence/united-nations-data-breach-started-with-microsoft-sharepoint-bug

NVD - cve-2019-0604. (n.d.). https://nvd.nist.gov/vuln/detail/cve-2019-0604

Souppaya, M., & Scarfone, K. (2022b). *Guide to enterprise patch management planning:* https://doi.org/10.6028/nist.sp.800-40r4

Souppaya, M., & Scarfone, K. (2013). *Guide to Enterprise Patch Management Technologies*. https://doi.org/10.6028/nist.sp.800-40r3

Scarfone, K. A., & Mell, P. M. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. https://doi.org/10.6028/nist.sp.800-94

Barker, E., & Barker, W. C. (2019). *Recommendation for key management:* https://doi.org/10.6028/nist.sp.800-57pt2r1

Security and privacy controls for information systems and organizations. (2020). https://doi.org/10.6028/nist.sp.800-53r5

Stouffer, K. (2023). *Guide to Operational Technology (OT) security*.

https://doi.org/10.6028/nist.sp.800-82r3