Investigation & Research Report

Subject:

United Nations Data Breach

Robert Ajegbo

Lighthouse Labs Cyber Security June 26 Cohort

Week 8 Threat Defense Project

Table of Contents:

1. Executive Summary:

If there is one thing that is clear in this global; digital age, it is that just about anyone and anything can be the target of a cyber attack. That group of possible targets includes everything from individuals and small businesses all the way up to large organizations and entire governments. An example of these attacks on a major organization was the 2019 data breach against the United Nations (or UN for short). The UN is an international organization currently made of 193 member states in alliance to promote global peace and cooperation through diplomacy, humanitarian efforts, and the resolution of conflicts.

In this report, I will dive deeper into the details about the data breach that they suffered. I will look to uncover information such as how the incident occurred and how it could have been prevented.

2. **Who were the victims of the attacks?**

The breach affected the United Nations and a large number of their associated organizations. The data accessed by the hackers included a wide range of sensitive data pertaining to employees associated with the company. This included personal and professional information of thousands of staff, and their login credentials also.
With confidential data like this exposed to hackers and attackers, the organization's staff could be left vulnerable to risks such as identity theft and financial losses. It also puts the companies involved at risk of privacy violation, reputational damage, and operational disruption.

3. **What technologies and tools were used in the attack?**

The hackers conducted this attack by exploiting a bug in Microsoft SharePoint. This was due to a critical remote code execution vulnerability that allowed the attackers to gain remote access to the UN's servers. Microsoft had released a security patch for the vulnerability prior but the IT staff did not update the software in time which left the systems vulnerable to the hackers. You can find more information about the vulnerability exploited (CVE-2019-0604) below.

CVE-2019-0604 Detail

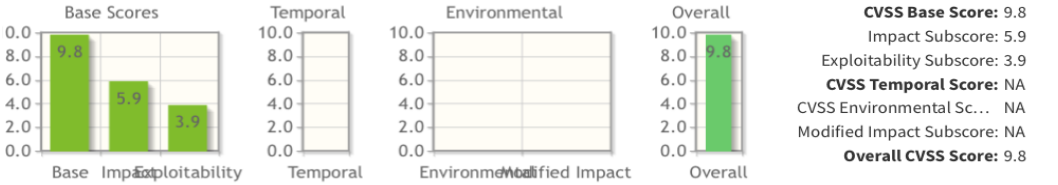
Description

A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0594.

Common Vulnerability Scoring System Calculator CVE-2019-0604

Source: NIST

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

4. **What systems were targeted?**

At first, it was unclear when the breach had occurred due to the fact that the United Nations tried to hide the attack from the public. It was later revealed in leaked confidential reports that the attack began in July of 2019. There were 42 servers in total that were all confirmed to be compromised and another 25 that were categorized as suspicious. Some of the affected systems were from the human rights department in Geneva and some others were believed to be from human resources departments in both Geneva and Vienna. The core infrastructure affected included systems for user and password management, system controls, and security firewalls.

5. **What was the motivation of the attackers?**

It has not been confirmed who the specific hackers are and what their motivation for the attack was. However, given the contents of the data that they stole; it would be a fair assumption to say that they may have stolen the data to plan for a more significant attack on the United Nations or they may intend to target individual employees through other methods of cyber incidents. It could also be a type of reconnaissance or espionage tactic used by non-member states to find further vulnerabilities in the UN systems.

6. **What was the outcome of the attack?**

As stated above, the attack was a result of the hackers exploiting a bug in some software and they managed to steal an estimated 400 GB of data. This data came from 42 compromised servers from various UN offices and it included the personal data of employees. It is unclear as to what confidential data was included for each individual but it includes directories that could contain staff records, health insurance systems and other resources. This kind of information in the wrong hands can threaten the privacy of these people and potentially leave them at risk of other attacks. This was not the only damage done however, as the United Nations made the mistake of trying to keep everything a secret and did not disclose any information of the breach. It was revealed that the employees were only told to change their passwords but they did not get any further details. This may not have been a breach in any laws but it most definitely would call the organization's integrity into question and may damage their reputation and result in a loss of trust from their employees that were victims. The fact that they were left oblivious to the attack could have

left them significantly vulnerable to follow up attacks such as comprehensive phishing attempts using their own private information.

7. **Recommended mitigation techniques and security controls to prevent future attacks:**

In the case of the United Nations Data Breach, there was clear negligence in the case of the IT team that should have ensured that the systems were regularly updated with security patches. However, this is not the only step that organizations can and should take to mitigate these risks. Below I will list some effective strategies that can be taken to try and prevent future cyber attacks.

Conduct a cybersecurity risk assessment

This can help to uncover potential vulnerabilities in your organization's infrastructure so that you can bolster protection and limit the risks.

Network Segmentation

Isolate your critical systems and sensitive data from less secure areas.

Limit and control account access

You should only grant users and systems the minimum access needed to perform their tasks.

Multi-factor authentication

Always use multi factor authentication to ensure that potential stolen credentials are backed up by another layer of protection.

Encryption

Make sure that all sensitive data is encrypted so that only authorized parties can read it even if the data is stolen.

Regular Employee Training

It is important to ensure that all employees are made aware of the importance of keeping their data safe and protecting the organization. In some cases, it only takes one naive user to breach an entire company's database through phishing and other attacks.

Create a Secure Cybersecurity Policy

Should include plans for disaster recovery, security testing, and incident response.

Deploy the assistance of a third-party cyber security team

A cyber security team can help to monitor the organization's systems and networks for any abnormal behaviour and respond to incidents in an efficient manner.

References

CVE-2019-0604. (n.d.). MSRC portal. Retrieved August 21, 2023, from https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0604

Dark Reading Staff. (2020, January 31). *United Nations Data Breach Started with Microsoft SharePoint Bug*. Dark Reading. Retrieved August 21, 2023, from https://www.darkreading.com/threat-intelligence/united-nations-data-breach-started-with-microsoft-sharepoint-bug

Jackson, M. (2021, February 10). *Data Breach Review of United Nations*. GitGuardian Blog. Retrieved August 21, 2023, from https://blog.gitguardian.com/united-nations-databreach-jan/

LIFARS. (2021, October 4). *Data Breach: Attackers Breached Systems of United Nations*. LIFARS.com. Retrieved August 21, 2023, from https://www.lifars.com/2021/10/data-breach-attackers-breached-systems-of-united-nations/

Matthews, K. (2020, February 7). *Incident Of The Week: Leak Discloses UN Data Breach From 2019*. Cyber Security Hub. Retrieved August 21, 2023, from https://www.cshub.com/attacks/articles/incident-of-the-week-leak-discloses-un-2019-breach-from-2019

NVD - CVE-2019-0604. (2019, March 5). NVD. Retrieved August 21, 2023, from https://nvd.nist.gov/vuln/detail/CVE-2019-0604

Parker, B. (2020, January 29). *EXCLUSIVE: The cyber attack the UN tried to keep under wraps*. The New Humanitarian. Retrieved August 21, 2023, from

https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack

PERSONNEL BY ORGANIZATION. (n.d.). United Nations - CEB. Retrieved August 21, 2023, from https://unsceb.org/hr-organization

Researching Cyber Security Attack. (2019, March 9). LHL Compass. Retrieved August 21, 2023, from https://cyber.compass.lighthouselabs.ca/p/2/days/w08d3/activities/3059

Sen, K. (2023, July 4). *10 Ways to Reduce Cybersecurity Risk for Your Organization*. UpGuard. Retrieved August 21, 2023, from https://www.upguard.com/blog/reduce-cybersecurity-risk#toc-0

Steinbrecher, D. (2022, May 6). *UN data breach (2021) - International cyber law: interactive toolkit*. Cyber Law Toolkit. Retrieved August 21, 2023, from https://cyberlaw.ccdcoe.org/wiki/UN_data_breach_(2021)

Threat Defense Investigation & Research Report. (2019, March 9). LHL Compass. Retrieved August 21, 2023, from https://cyber.compass.lighthouselabs.ca/p/2/days/w08d3/activities/3058

12 Tips for Mitigating Cyber Risk | JPMorgan Chase. (2022, September 29). J.P. Morgan. Retrieved August 21, 2023, from https://www.jpmorgan.com/insights/cybersecurity/ransomware/12-tips-for-mitigating-cyber-risk

United Nations. (n.d.). *About Us | United Nations*. the United Nations. Retrieved August 19, 2023, from https://www.un.org/en/about-us

Winder, D. (2019, March 9). *United Nations Confirms 'Serious' Cyberattack With 42 Core Servers Compromised*. Forbes. Retrieved August 21, 2023, from https://www.forbes.com/sites/daveywinder/2020/01/30/united-nations-confirms-serious-cyberattack-with-42-core-servers-compromised/?sh=42cf9842633d

Writing Investigation & Research Report. (2022, October 2). LHL Compass. Retrieved August 21, 2023, from https://cyber.compass.lighthouselabs.ca/p/2/projects/research-report?day_number=w08d4

Zorz, Z. (2020, January 30). *UN hacked: Attackers got in via SharePoint vulnerability*. Help Net Security. Retrieved August 21, 2023, from https://www.helpnetsecurity.com/2020/01/30/un-hacked/