AL2024_28 High-Severity Vulnerability in Microsoft Office Exposes NTLM Hashes (August 13, 2024)

Description

On August 9, 2024, Microsoft disclosed a high-severity vulnerability in Microsoft Office, tracked as CVE-2024-38200, which could expose NT LAN Manager (NTLM) hashes to a remote attacker. This flaw affects multiple versions of Microsoft Office, including Office 2016, Office 2019, Office LTSC 2021, and Microsoft 365 Apps for Enterprise. The vulnerability stems from an information disclosure weakness that allows unauthorized actors to access protected information.

While Microsoft's initial assessment suggested that exploitation of this vulnerability is less likely, MITRE has identified the likelihood of exploitation as highly probable. The vulnerability could be exploited through a web-based attack scenario, where an attacker hosts a website containing a specially crafted file designed to exploit the flaw. Users must be convinced to click on a link and open the file, typically delivered via email or instant messaging.

Attack Details

The **CVE-2024-38200** vulnerability allows attackers to initiate an outbound NTLM connection from a victim's system to a remote server controlled by the attacker. When this connection occurs, Windows automatically sends the user's NTLM hashes, including the hashed password, to the attacker's server. These hashes can be cracked, enabling threat actors to gain access to login names and plaintext passwords.

The vulnerability could also facilitate NTLM Relay Attacks, a method previously demonstrated in attacks like ShadowCoerce, DFSCoerce, PetitPotam, and RemotePotato0. These attacks allow threat actors to gain access to other resources on a network by leveraging the NTLM hashes.

Microsoft has acknowledged the seriousness of this vulnerability and is actively working on security updates to address it. A partial fix was enabled via Feature Flighting on July 30, 2024, protecting customers on all in-support versions of

Microsoft Office and Microsoft 365. A final fix is expected in the August 13, 2024, updates.

Remediation

To mitigate the risk associated with CVE-2024-38200, Microsoft recommends several actions:

1. **Block Outbound NTLM Traffic**: Configure Network Security to restrict NTLM: by changing this setting stops Windows computers (like Windows 7 or Windows Server 2008) from sharing sensitive information (NTLM) with other computers. This helps protect your network from potential security risks.
2. **Protected Users Security Group**: Add users to the Protected Users Security Group, which restricts the use of NTLM as an authentication mechanism.
3. **Block TCP Port 445**: Block all outbound traffic to TCP port 445, which is commonly used for SMB (Server Message Block) communications and could be exploited in this context.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Gatlan, S. (2024, August 10). Microsoft discloses unpatched Office flaw that exposes NTLM hashes. Retrieved from *BleepingComputer*.

https://www.bleepingcomputer.com/news/security/microsoft-discloses-unpatched-office-flaw-that-exposes-ntlm-hashes/

- Vulnera. (2024, August 9). *Unpatched Microsoft Office flaw could expose NTLM hashes - VULNERA*. Retrieved from VULNERA - Vulnerability Management. Simplified. https://vulnera.com/newswire/unpatched-microsoft-office-flaw-could-expose-ntlm-hashes/