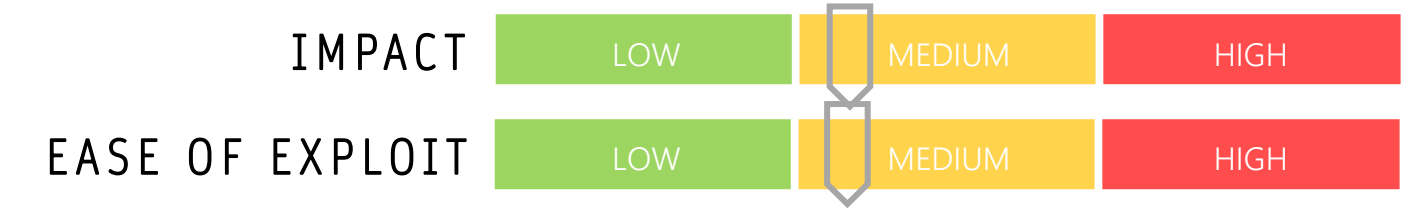
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00018

MICROSOFT TEAMS PATCH BYPASS

DATE ISSUED: 5th August 2020



OVERVIEW

With a massive shift to video conferencing and communication with the presence of Covid-19, attackers have taken advantage of increased usage to take the opportunity to use updates and a vehicle for malicious payloads – which is the case with the Microsoft Teams application.

BREAKDOWN

With such a high volume of updates to the popular Microsoft Teams application during the elevated use throughout the global pandemic, Microsoft attempted to remove the ability of malicious actors to insert malware by restricting Teams to be updated by URL only. This band-aid solution may be bypassed using Service Message Blocks (SMB) by dropping a malicious file into an open shared folder, which would normally require the user to already have network access, although it has been discovered that a remote share can perpetuate the same result. This type of attack utilises 'Samba' to carry out remote downloading for the Microsoft Teams Updater and once setup is complete, Remote Code Execution (RCE) and lateral movement throughout the system is then possible.

REMEDIATION STEPS

- Monitor network logs for unusual activity such as unauthorised in-bound or out-bound connections
- Have the internal IT team install Microsoft Teams under Program Files preventing remote drop and execution of remote payloads using a Group Policy
- Disable automatic push update mechanisms and perform all updates via internal IT team processes

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/microsoft-teams-patch-bypass-rce/158043/
Dark Reading https://www.darkreading.com/attacks-breaches/microsoft-teams-vulnerable-to-patch-workaround-researchers-report/d/d-id/1338583
Microsoft Tech Community https://techcommunity.microsoft.com/t5/microsoft-teams/teams-updater-vulnerability/m-p/724492