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

CYBER GUIDANCE ISSUE 0334

MICROSOFT TEAMS BUG ALLOWS MALWARE DELIVERY

DATE ISSUED: 28th June 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

Researchers found a way to deliver malware through Microsoft Teams, bypassing security controls and tricking the system into treating external users as internal. This enables the delivery of malicious payloads disguised as downloadable files.

BREAKDOWN

Security researchers from Jumpsec have discovered a way to deliver malware using Microsoft Teams with an account outside the target organisation. The attack begins with Microsoft Teams running the default configuration that allows communication with Teams accounts outside the company (external tenants). While external users (tenants) are initially restricted from sending files to employees of different organisations, it has been discovered that the client-side security controls preventing this can be circumvented. By modifying the recipient IDs in the POST request of a message, both for internal and external users, it becomes possible to deceive the system into treating an external user as if they were an internal user. This allows the external tenant/attacker to send a malicious payload that will appear in the target's inbox as a file for download. This approach cleverly evades almost all contemporary anti-phishing security measures, specifically those pertaining to email safeguards.

REMEDIATION STEPS

- Raise awareness among employees about the potential for attackers to exploit productivity applications like Teams, Slack, or SharePoint as platforms for carrying out social engineering attacks.
- Disable the feature of communication with external tenants from "Microsoft Teams Admin Center>External Access".
- Organisations can establish an allow-list by defining specific domains, ensuring that only authorised external communication channels are maintained.
- Practice the Principle of Least Privilege on all systems and services to lower the risk of attacks.

REFERENCES & RESOURCES

Help Net Security https://www.helpnetsecurity.com/2023/06/23/microsoft-teams-deliver-malware/

Bleeping Computer https://www.bleepingcomputer.com/news/security/microsoft-teams-bug-allows-malware-delivery-from-external-accounts/