SECURITY CHALLENGES IN VIDEO CONFERENCING APPLICATIONS: A CASE STUDY ON MICROSOFT TEAMS

CZU: 004.056:004.738.52
DOI: https://doi.org/10.53486/tids2026.31

AURELIU ZGUREANU
Academy of Economic Studies of Moldova (ASEM)
e-mail: zgureanu.aureliu@ase.md
ORCID ID: 0000-0003-3301-2457

SERGHEI OPREA
Academy of Economic Studies of Moldova (ASEM)
e-mail: oprea.serghei@ase.md
ORCID ID: 0000-0003-3759-8598

Abstract. The rapid expansion of remote work and digital collaboration has positioned video conferencing platforms at the centre of organisational communication infrastructure. Microsoft Teams, with over 320 million monthly active users across more than one million organisations worldwide, has become a primary target for a wide spectrum of cyber threats. This paper investigates the security challenges inherent to video conferencing applications, with a focused case study on Microsoft Teams app. The research examines the threat landscape through five interconnected dimensions: technical vulnerabilities exploitable at the protocol and application layer; social engineering and phishing campaigns exploiting user trust within the platform; data privacy risks arising from inadequate encryption, misconfigured permissions, and insecure third-party integrations; regulatory compliance challenges under frameworks such as the GDPR and HIPAA and the human factors that amplify technological vulnerabilities. Based on peer-reviewed academic literature, official Microsoft security documentation, threat intelligence reports from organisations including Check Point Research and Microsoft DART, and disclosed CVE records, the paper constructs a comprehensive threat taxonomy. Specific attack techniques examined include the GIFShell attack chain enabling covert data exfiltration through legitimate Microsoft infrastructure, remote code execution vulnerabilities triggered via adversary-crafted meeting invitations, identity spoofing through webhook payload manipulation, and state-sponsored social engineering campaigns attributed to the Midnight Blizzard threat actor. The paper further analyses the permission escalation risks within the Teams add-on ecosystem and the privacy side-channels introduced by virtual backgrounds and auxiliary devices. The findings reveal that the security posture of Microsoft Teams is compromised not solely by software defects but by systemic design trade-offs that prioritise usability and interoperability. Mitigation recommendations include technical hardening measures, governance frameworks, and user education programmes. This research contributes to the growing body of knowledge on enterprise collaboration platform security and provides practitioners with actionable guidance for securing video conferencing environments.

Keywords: Microsoft Teams, video conferencing security, cybersecurity, social engineering, data privacy, GDPR compliance.

JEL Classification: M15, K24, O33.

INTRODUCTION

The COVID-19 pandemic beginning in early 2020 sped up the use of video call platforms in most industries, including education, healthcare, government, and the private sector. What had once been a temporary solution became critical. Microsoft Teams became one of the major platforms during this time. Its rise was facilitated by the deep integration of the Microsoft 365 suite and its

business tools. By 2024, Microsoft Teams reached over 320 million daily active users, greatly increasing its strategic importance, and its attractiveness as a target by threat actors. (Charikov and Vanunu, 2025).

Research into security issues on different video conferencing platforms expanded significantly. Kagan *et al.* (2020) demonstrated that malicious actors could exploit publicly accessible meeting links to collect biometric data from unsuspecting participants. This data may include facial images, voice samples, and other types of data. The authors also showed that deep-learning algorithms could be used to identify a person in others different meetings, raising severe privacy issues. Alammary *et al.* (2022), used the Knowledge-Attitudes-Behaviours mode to survey data from 307 faculty members across 43 different universities in Saudi Arabia. Then they showed that the level of video conference security settings is "poor" and emphasizes the human factor as the most significant vulnerability. The threat modelling study published by Hasan and Hasan (2022) used the widely known STRIDE framework - Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege - on different video conferencing tools and effectively constructed an exhaustive list of risk categories applicable directly also to Teams.

Microsoft Teams continues to be a popular tool within organizations worldwide, thus, suggesting a need for continued research and security assessments.

Bobby Rauch revealed the GIFShell attack chain on September 2022, which showed that by chaining together seven vulnerabilities in Microsoft Teams, a covert reverse shell could be created that exfiltrated commands and data via Microsoft's own infrastructure (Rauch, 2022). Microsoft released fixes for CVE-2023-29328 and CVE-2023-29330 in August 2023, both of which are critical remote code execution vulnerabilities that could be exploited by getting a target user to join an adversary's Teams meeting (Munshaw, 2023). Additionally, Charikov and Vanunu (2025) identified a series of notification manipulation and message spoofing vulnerabilities that allow for identity impersonation on the Teams platform, which are officially tracked as CVE-2024-38197. In parallel, Microsoft's threat intel revealed that APT29, a state-funded Russian threat actor, used Teams as a channel for a spear-phishing attack to obtain credentials from government and critical infrastructure organizations (Intelligence, M.T., 2023).

This paper provides an analysis of Microsoft Teams security - the technological vulnerabilities, threat analysis, and industry compliance frameworks. It aims to lay down the imperative security challenges posed by Microsoft Teams within an evidence-based analytical framework. The analysis of the security challenges posed by Microsoft Teams will be broken down into implicit threat actors and APT analysis, various attack mechanisms and their relative effectiveness, the severity of violation and defensive mechanisms in place, and technical and non-technical solutions to address the security challenges in a vertical and horizontal stance.

MAIN CONTENT

1. Platform Architecture and Security Model

Microsoft Teams is built on Microsoft 365's hyper-scale cloud platform, combining proprietary protocols and standard protocols. Secure Real-time Transport Protocol (SRTP) is used to deliver audio and video streams, and all data in transit is encrypted and protected by Transport Layer Security (TLS). Data in Microsoft's data centers is secured by BitLocker, and any files in OneDrive or SharePoint inherit the encryption schemes of those services. The application's desktop client is built on Electron, a framework that embeds a Chromium-based browser engine to render web technologies

as native desktop applications. This architectural option presents the most important security risk. Electron does not enforce encrypted or protected file storage by default, meaning that local Teams log files - which may contain session tokens and sensitive metadata - are accessible to any process running under the user's account. This exposure was a foundational prerequisite for the GIFShell attack. (Keusseyan, 2024). This Security flaw was a founding condition of the GIFShell assault. Microsoft Teams uses Azure AD as the primary provider, and Microsoft provides authentication mechanisms that are required by the platform. All authentication mechanisms are based on the OpenID Connect and OAuth 2.0 processes. This creates the option for, and in some cases the obligation for implementers to use, multi-factor authentication. Azure AD creates the conditions for Microsoft Teams to have fine-grained control mechanisms.

Research made available in 2025 on arXiv showed that an automated testing tool dubbed TAI found 41 host APIs which can be manipulated by add-ons for permission escalation, thus allowing access to documents, spreadsheets, and shared drives that are outside the scope of the add-on's permissions.

2. Technical Vulnerabilities and Attack Techniques

The Microsoft Teams software can be attacked in various ways, but the most concerning of these involve RCE vulnerabilities, including CVE-2023-29328 and CVE-2023-29330. Munshaw (2023) says that both vulnerabilities allow an attacker to send a Teams meeting invite, and the recipient does not need to take any other action to participate in the meeting and thus be attacked, which significantly lower the barrier to exploit. Having an RCE vulnerability that does not require an attacker to pre-coordinate with a target or exploit a vulnerability on the target to gain a foothold is especially dangerous for RCE vulnerabilities in Microsoft Teams.

In 2022, Rauch introduced the GIFShell technique, which is a covert channel attack that allows the attacker to send text and lead the recipient to an attacker designated website using created API requests. This allows a user to bypass the Teams restriction on sharing outside of the Teams community and send a file to appear as benign images, Teams' retrieval of GIF images from attacker-controlled servers, and the embedding of executable commands within base64-encoded GIF filenames. Since the exfiltration pathway along with the telemetry traffic is a normal Teams traffic, the activity is unlikely to be flagged by EDR or other network monitoring systems. Microsoft said that the GIFShell technique is a post-exploitation technique and does not need an urgent fix (as of 2022, this technique is more or less a GIF hacking channel).

Table 1. Classification of Security Threats in Microsoft Teams

Threat Category	Attack Vector	Key CVE / Case Study
Remote Code Execution	Malicious meeting links	CVE-2023-29328, CVE-2023-29330
Identity Spoofing	Webhook payload forgery	CVE-2024-38197 (Check Point, 2025)
Data Exfiltration	GIF-embedded commands	GIFShell chain (Rauch, 2022)
Social Engineering	Cross-tenant vishing	Midnight Blizzard (Microsoft, 2023)
Privilege Escalation	Third-party add-on abuse	TAI tool findings (Wan et al, 2025)
Privacy Side-Channel	Virtual background instability	He & Lei (2021)

Source: *Compiled by the author based on Intelligence, M.T. (2023), Microsoft (2023b)*, *Microsoft (2026), Charikov and Vanunu (2025), Rauch (2022), Wan et al. (2025).*

Identity spoofing allows deception of users by having them believe a message has originated from a trusted contact. A technique of this kind of deception, described by Charikov and Vanunu (2025), is employing bots and webhooks to generate message payloads that falsify sender attributes. Check Point Research discovered that these bots and webhooks modified messages to appear as if they originated from Teams executives or other trusted users. The CVE-2024-38197 vulnerability has been classified with a medium severity rating. This classification suggests that some degree of attacker access is required to the organization's tenant. The researchers have, however, demonstrated a proof of concept that amplifies the risk of business email compromise (BEC) style activities in the Teams environment.

3. Social Engineering and Phishing via Microsoft Teams

Instead of short phishing messages, social engineering has developed into sophisticated intrusion campaigns. Midnight Blizzard, also known as APT29, Cozy Bear, and NOBELIUM, compromised multiple Microsoft 365 small business tenants and created domains to impersonate the Microsoft 365 technical support. Several messages were sent to the Microsoft 365 ‘Teams’ to the employees and contractors of the government and critical infrastructure, suggesting a type of support request to approve multi-factor authentication during an assumed Microsoft 365 technical support scenario. This, among others, is one of the campaigns described in the 2023 Microsoft Threat Intelligence report. The latest sophisticated campaign has also been revealed by the Microsoft Detection and Response Team during the 2026 Microsoft Threat Intelligence report. While DART was engaged to the customer in November 2025, a persistent voice phishing campaign through Microsoft 365 Teams was documented. Impersonating from the Microsoft 365 IT Helpdesk, the customer DART employees were called multiple times. The employees were prompted to open the Microsoft 365 Teams remote control feature; Quick Assist, from which the phishing Helpdesk was able to take full control of the devices, conduct reconnaissance, lateral movement and access the Microsoft 365 domains and the Windows Server domain controllers. Microsoft has also documented the activities of a group of fraudsters who referred to themselves as the UNC6692 group, during an April 2026 Microsoft Threat Intelligence Report. This group has also used a similar methodology as described above, but further advanced by creating and deploying a custom malware dubbed SNOW and a malicious browser extension.

According to Gogia's (Swain, 2026) description, this depicts a less traditional variety of phishing he describes as “guided execution.” In this variation, attackers prematurely integrate themselves into legitimate enterprise workflows for the purpose of guiding their victim to execute a series of actions that result in the granting of access permissions. He & Lei (2021) describe a more nuanced general social engineering threat. They describe the reality that virtual backgrounds in modern video conferencing solutions may not be entirely virtual, which may inadvertently compromise the physical social environment of the target that social engineering efforts are aimed at, revealing new information to the social engineer of potential.

4. Data Privacy and Regulatory Compliance

Microsoft Teams operates within a broad compliance ecosystem. Based on compliance with numerous regulatory frameworks, including HIPAA, GDPR, FedRAMP, SOC 1, SOC 2, and FERPA, Teams facilitates compliance with over 90 different regulations and laws. Microsoft includes Teams in compliance with regulations for GDPR, HIPAA, and FedRAMP, among others (Microsoft Pulse 2025). While Microsoft operates as a data processor for customers in GDPR compliance, Microsoft

provides Standard Contractual Clauses (SCCs) in place of GDPR compliance for cross-border data transfers from the European Economic Area (Microsoft (2023a), Microsoft (2023b)).

Implementing Teams to support compliance is only the first step, as there are considerable compliance related demands on the organization. The European Banking Authority (EBA 2025) Microsoft Teams Data Protection Notice describes the types of processed personal data. These data types consist of biometric data, voice and meeting recordings, etc. The transfer of sensitive data is prohibited without explicit user consent. One of the compliance gaps is that Microsoft 365 average retention is 30 to 90 days, however, regulated industries (mostly, financial services) have to comply with long retention (up to 7 years) requirements (FINRA 4511), and, as a result, require 3rd party archiving services (Clarke, 2025).

Data Compliance is complicated with various archiving requirements. While data is stored in the regional Microsoft 365 compliance instance, it is also persistently stored in multiple instances of compliance data in the Microsoft 365 ecosystem.

Organizations subject to stringent data sovereignty protocols - including (but not limited to) defence, health care, and government sectors - must assess their data residency setup and, if applicable, implement Microsoft Teams in government cloud (GCC) or sovereign cloud implementations. The assertion made by the GDPR that encryption is a consequence modifier for breach notifications speaks to and creates an argument for the necessity that all data pathways in Microsoft Teams be configured such that there is a strict adherence to encryption by way of the protocols TLS and SRTP (Microsoft Learn, GDPR, 2025).

5. Materials and Methods

This research adopts a qualitative systematic review framework to collate evidence across several categories: (1) peer-reviewed papers accessed through arXiv, PubMed Central, and publisher internet gateways, chosen for their relevance to security in online videoconferencing in general, and Microsoft Teams in particular; (2) exposed vulnerabilities in the Common Vulnerabilities and Exposures (CVE) database, along with patch Tuesday advisories; (3) threat intelligence reports from Microsoft's Detection and Response Team, Microsoft Threat Intelligence, and Check Point Research; (4) Microsoft's technical documentation located on Microsoft Learn and in The Microsoft Trust Centre; and (5) Microsoft's GDPR documentation and European Banking Authority regulatory documentation.

Sources were judged based on four characteristics: recency (sources published from March 2020 to the present for their relevance to the post-pandemic context), authoritativeness (published and peer-reviewed papers and reports from established security research organisations), relevance (applicability to Microsoft Teams and/or the security of video conferencing), and methodological rigor (research incorporating threat models, or experimental frameworks, or validated instruments). The STRIDE model of threat is utilized to construct the threat taxonomy illustrated in this paper, in accordance with the Hasan and Hasan (2022) study. The yield of this taxonomy is shown in Table 1.

6. Results and Discussion

The sources collectively demonstrate a complex threat scenario for Microsoft Teams comprising multiple technical, human, and regulatory layers. The technical threat derives from the Electron-based desktop client, which creates a persistent attack surface that still requires constant vigilance even if the code is patched. Electron prioritizes platform bridging for the sake of convenience over containing the filesystem, which is the underlying root of the desktop client attack surface. The reemergence of RCE vulnerabilities in the meeting subsystem (CVE-2023-29328, CVE-

2023-29330) signifies a sustained challenge in containing an untrusted input that is capable of exploiting the meeting subsystem and other complex media processing pipelines.

From a human perspective, the combination of two trends poses a notable threat. The first is the declining notion of an "inside versus outside" boundary of communications in the context of Teams. The second is social engineering, in which exploitation of this boundary is becoming systematically more complex. As Kaur (Swain, 2026) noted, collaboration platforms that enable real-time interaction allow for a more believable and actual instance of an IT personnel impersonation in comparison to more traditional email-based phishing. The interaction, in this instance, takes place in a channel that users implicit trust toward Teams and collaboration platform communications. This finding corroborates the low usability awareness scores attained by Alammary et al. (2022), signifying that user training in and of itself is insufficient.

While vendor threat modelling, in general, is characterized by distinctive limitations, the GIFShell experiment is a particularly appropriate and illustrative example of such limitations. Microsoft's definition of the GIFShell attack is a post-exploitation technique that lies outside the vendor's concerns for "immediate" or "near-term" mitigation. This post hoc evaluation of the attack is the result of a low contextual security boundary that fails to capture the cumulative nature of the risk that follows from multiple rounds of design violations of a low company security threshold.

From a risk management viewpoint, we should assess the likelihood of threat actors capitalizing on a particular vulnerability, as opposed to the single, arbitrary severity of a vulnerability. Here, the likelihood is, indeed, affirmative.

The disagreement in the privacy regulatory layer is once more the distance of Microsoft's assurances of compliance and the real compliance Microsoft achieves. The GDPR mandates that the organisational customer that deploys Microsoft Teams must, among other things, appoint a Data Protection Officer, issue privacy notices, and carry out and maintain Records of Processing Activities. The EBA's formal data protection notice for Teams illustrates this point: even a sophisticated financial regulator requires a dedicated legal instrument to govern its own use of the platform.

CONCLUSIONS

This work provided an insight into the Microsoft Teams platform and its most critical security issues when using video conferencing software. The evidence demonstrates that the platform's threat landscape encompasses technical vulnerabilities at the application and framework layers, sophisticated social engineering campaigns conducted by both cybercriminal and state-sponsored threat actors, data privacy risks arising from design trade-offs and third-party integrations, and significant organisational compliance burdens under major data protection regulatory frameworks.

The novelty of this research lies in its integrative approach, combining CVE-level technical analysis, security psychopathy of active threats, and regulatory compliance frameworks to form an integrated and unified threat taxonomy. Additionally, it provides fundamental evidence against the hypothesis which suggests enterprise-level video conferencing software that provides substantial compliance frameworks is secure. Also, security posture is the outcome of a combination of a user's deployment structure, behaviour, and governance as a regulation.

This work recommends an integrated view of security posture at the philosophy level which mainly includes the extensibility of policy and technical control to address the gaps in framework security posture.

- Technical control options include disallowing inter-tenant communication, deactivation of Quick Assist, enacting SMB signing, enforcement of MFA, and removal of remote access;
- Policy control options include implementation of DLP frameworks and defining retention schedules;
- Programs to educate users on the risks of Teams social engineering;
- Comprehensive oversight of Teams users to increase ID access control via adjustment of Security Information Event Management (SIEM) structures to allow for the oversight and control of foreign access.

Future research directions include longitudinal analysis of the effectiveness of user training interventions in reducing Teams-based social engineering susceptibility, empirical evaluation of the security impact of the new Teams client architecture released in 2024, and comparative analysis of security postures across competing enterprise collaboration platforms. A limitation of this study is its reliance on publicly disclosed vulnerabilities and threat intelligence; zero-day vulnerabilities actively exploited in the wild remain, by definition, uncharacterised in the open literature.

REFERENCES

Alammary, A., Alshaikh, M. and Pratama, A.R. (2022). Awareness of security and privacy settings in video conferencing apps among faculty during the COVID-19 pandemic. *PeerJ Computer Science*, 8, p.e1021. doi:https://doi.org/10.7717/peerj-cs.1021.

Charikov, A. and Vanunu, O. (2025). *Exploiting Microsoft Teams: Impersonation and Spoofing Vulnerabilities Exposed Microsoft Teams Vulnerabilities Uncovered*. [online] Check Point Research. Available at: https://research.checkpoint.com/2025/microsoft-teams-impersonation-and-spoofing-vulnerabilities-exposed/.

Clarke, J. (2024). *Microsoft Teams Compliance: GDPR, FINRA*. [online] Global Relay. Available at: https://www.globalrelay.com/resources/the-compliance-hub/compliance-insights/mirosoft-teams-compliance-gdpr-finra/.

European Banking Authority (EBA) (2025). *Privacy notice on processing personal data in Microsoft Teams*. [online] Available at: https://eba.europa.eu/sites/default/files/document_library/General%20Pages/Legal%20notice%20page/930896/Data%20Protection%20Notice%20on%20the%20Use%20of%20Microsoft%20Teams.pdf.

Hasan, R. and Hasan, R. (2022). Threat model and security analysis of video conferencing systems as a communication paradigm during the COVID-19 pandemic. In: *Novel AI and Data Science Advancements for Sustainability in the Era of COVID-19*. [online] Academic Press, pp.181–199. doi:https://doi.org/10.1016/b978-0-323-90054-6.00009-x.

He, S. and Lei, Y. (2021). *The privacy protection effectiveness of the video conference platforms' virtual background and the privacy concerns from the end-users*. [online] arXiv.org. Available at: https://arxiv.org/abs/2110.12493 [Accessed 29 Apr. 2026].

Intelligence, M.T. (2023). *Midnight Blizzard conducts targeted social engineering over Microsoft Teams*. [online] Microsoft Security Blog. Available at: https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/.

Kagan, D., Alpert, G.F. and Fire, M. (2020). Zooming Into Video Conferencing Privacy and Security Threats. *arXiv:2007.01059 [cs]*. [online] Available at: https://arxiv.org/abs/2007.01059.

Keusseyan, R. (2024). *Public Security Announcement: Microsoft Teams Vulnerabilities*. [online] Isec7.com.

Available at: https://blog.isec7.com/en/public-security-announcement-microsoft-teams-vulnerabilities [Accessed 29 Apr. 2026].

Microsoft (2023a). *General Data Protection Regulation - Microsoft GDPR*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr.

Microsoft (2023b). *Overview of security and compliance - Microsoft Teams*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/microsoftteams/security-compliance-overview.

Microsoft (2026). *Cross-tenant helpdesk impersonation to data exfiltration: A human-operated intrusion playbook | Microsoft Security Blog*. [online] Microsoft Security Blog. Available at: https://www.microsoft.com/en-us/security/blog/2026/04/18/crosstenant-helpdesk-impersonation-data-exfiltration-human-operated-intrusion-playbook/ [Accessed 29 Apr. 2026].

Microsoft Pulse. (2020). *Our commitment to privacy and security in Microsoft Teams*. [online] Available at: https://pulse.microsoft.com/en/work-productivity-en/na/fa2-our-commitment-to-privacy-and-security-in-microsoft-teams/.

Munshaw, J. (2023). *Six critical vulnerabilities included in August's Microsoft security update*. [online] Cisco Talos Blog. Available at: https://blog.talosintelligence.com/patch-tuesday-august-2023/ [Accessed 28 Apr. 2026].

Rauch, B., 2022. *GIFShell — covert attack chain and exfiltration via Microsoft Teams GIFs*. Medium/BleepingComputer disclosure, September 2022.

Swain, G. (2026). *Attackers abuse Microsoft Teams to impersonate the IT helpdesk in a new enterprise intrusion playbook*. [online] CSO Online. Available at: https://www.csoonline.com/article/4160858/ [Accessed 28 Apr. 2026].

Wan, L., Yan, C., Meng, M.H., Wang, K., Wang, H., Bai, G. and Dong, J.S. (2025). *Beyond the Scope: Security Testing of Permission Management in Team Workspace*. [online] arXiv.org. Available at: https://arxiv.org/abs/2506.17317 [Accessed 28 Apr. 2026].