Incidente ID:	0014
Fecha del reporte:	14/11/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad de suplantación de identidad en Microsoft Teams
Herramienta de detección	N/A
Activo involucrado:	Microsoft Team para iOS
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre las vulnerabilidades de Microsoft Teams que permiten a los atacantes suplantar la identidad de los usuarios y editar mensajes sin ser detectados.

Descripción:

Investigadores de seguridad de Check Point Research revelaron un conjunto de vulnerabilidades en Microsoft Teams que podían comprometer la integridad y la confianza en la plataforma de colaboración. Estas vulnerabilidades permiten que un atacante manipule el contenido de los mensajes sin que apareciera la etiqueta de "Editado", lo que da la impresión de que el remitente original sigue siendo legítimo. Además, era posible modificar las notificaciones entrantes de chat o llamada para que muestren un remitente fraudulento, como un directivo de la Entidad, con el fin de persuadir al usuario a abrir enlaces maliciosos o divulgar información sensible. También se descubrió que un atacante podía cambiar el nombre visible de los participantes en chats privados o alterar el tema de una conversación, facilitando la suplantación de identidad incluso en entornos de llamadas internas. Estas vulnerabilidades afectan tanto a usuarios internos como a invitados externos, ampliando significativamente la superficie de ataque.

La vulnerabilidad principal fue identificada con el CVE-2024-38197, con un puntaje CVSS de 6.5, que afecta la versión de Teams para inicialmente para iOS, aunque se confirmó que las implicaciones podían extenderse a otras plataformas. Microsoft informó que comenzó a desplegar las correcciones en agosto

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

de 2024 y continuó con parches adicionales en septiembre de 2024 y octubre de 2025. El impacto de estas vulnerabilidades radica en que socavan la confianza en la identidad de los mensajes dentro del entorno corporativo, permitiendo a los atacantes hacerse pasar por usuarios o superiores para ejecutar ataques de ingeniería social, distribuir malware o extraer información confidencial.

Productos afectados:

Aplicación de Teams para iOS: versiones hasta 6.19.2

Modo de explotación

La explotación no depende de un único exploit de ejecución remota sino de abuso lógico de las funciones de mensajería y notificación de Teams: un atacante puede reutilizar identificadores de mensaje y campos de notificación para modificar el contenido mostrado, ocultar que un mensaje fue editado, o suplantar el remitente en notificaciones mostrando a un directivo como origen. Estas manipulaciones pueden realizarse contra usuarios internos y cuentas de invitado, y se pueden usar como vector para inducir a víctimas a interactuar con enlaces o archivos maliciosos.

Recomendaciones de mitigación:

Aunque la vulnerabilidad afecta principalmente a la aplicación Microsoft Teams para iOS, se recomienda actualizar a la última versión disponible en todas las plataformas (Windows, macOS, Android y web) con el fin de garantizar la mitigación completa y mantener la coherencia de seguridad en el entorno colaborativo de Microsoft 365.

1- Actualización de versiones

- Instalar la última versión disponible de Teams en todas las plataformas (Windows, macOS, iOS, Android y web).

  Enlace de descarga oficial Windows escritorio
  https://www.microsoft.com/es-co/microsoft-teams/download-app

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- En iOS, actualizar a una versión 7.13.0 o superior
  Descargar versión desde la tienda oficial de App Store

2- Restringir la carga de archivos y enlaces externos

- Deshabilitar o limitar temporalmente la recepción de archivos desde usuarios externos o no autenticados hasta confirmar la actualización de seguridad.

- Configurar políticas de seguridad en Teams para impedir la vista previa automática de archivos o mensajes de remitentes externos.

3- Monitorear actividad anómala en Teams

- Revisar logs de actividad y auditoría en Microsoft 365 Defender o Microsoft Purview, especialmente intentos de acceso a través de mensajes o enlaces sospechosos.

4- Capacitación al personal

- Informar a los usuarios sobre la existencia de esta vulnerabilidad y reforzar las políticas de no abrir archivos ni enlaces inesperados incluso si provienen de usuarios aparentemente conocidos.

5- Mantener los parches de seguridad al día

- Asegurar que las actualizaciones automáticas de Teams y del entorno Microsoft 365 estén habilitadas.

Fuentes:

- https://research.checkpoint.com/2025/microsoft-teams-impersonation-and-spoofing-vulnerabilities-exposed/?utm_source

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- https://blog.checkpoint.com/research/exploiting-trust-in-collaboration-microsoft-teams-vulnerabilities-uncovered/?utm_source
- https://dbugs.ptsecurity.com/vulnerability/CVE-2024-38197?utm_source
- https://thehackernews.com/2025/11/microsoft-teams-bugs-let-attackers.html?utm_source

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570