JMSSA2026-001：
LiveOn Meet の Windows PC用クライアントインストーラおよびプラグインインストーラにおける任意の DLL 読み込みの脆弱性

公開日 2026 年 4 月 21 日
最終更新日 2026 年 4 月 21 日

■概要

LiveOnMeet の WindowsPC用LiveOnMeet クライアントインストーラおよびキヤノンネットワークカメラ用プラグインインストーラの特定バージョンに、DLL 読み込み時の検索パスに関する脆弱性が存在することが判明しました。

この脆弱性を悪用された場合、インストーラと同一フォルダに攻撃者が用意した特定の DLL が読み込まれ、悪意ある第三者によって任意のコードが実行される危険性があります。

本脆弱性はインストーラの実行時にのみ発生します。既にインストールを完了されているお客様については LiveOnMeet を引き続き安全にご利用いただけますので、アンインストールを行う必要はございません。

影響を受けるバージョンのインストーラをお持ちのお客様は必ず PC から削除してください。

■該当製品の確認方法

影響を受ける製品は以下のとおりです。

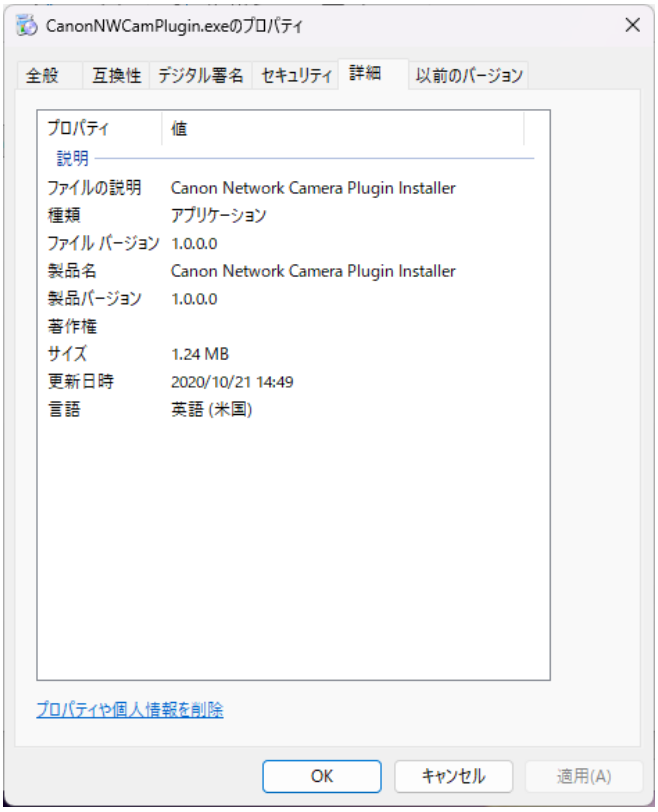
製品名称　　：LiveOnMeet クライアントインストーラ
対象アプリケーション：Downloader5Installer.exe
　　Downloader5InstallerForAdmin.exe
該当バージョン　　：Ver.1.0.0.0

製品名称　　：キヤノンネットワークカメラ用プラグインインストーラ
対象アプリケーション：CanonNWCamPlugin.exe
　　CanonNWCamPluginForAdmin.exe
該当バージョン　　：Ver.1.0.0.0

お使いのバージョンの確認方法は以下のとおりです。

1. ダウンロードしたインストーラのファイルを右クリックし、「プロパティ」を選択

2. 「詳細」タブを開き、「ファイルバージョン」の項目を確認



■脆弱性の説明

LiveOnMeet の WindowsPC用LiveOnMeet クライアントインストーラおよびキヤノンネットワークカメラ用プラグインインストーラは、インストール処理の際に特定の DLL を読み込む機能を備えています。 しかし、当該インストーラには DLL 読み込み時の検索パスの処理に問題があり、インストーラと同一フォルダに存在する特定の DLL を読み込んでしまう脆弱性が存在します。 これにより、攻撃者が用意した悪意のある DLL が意図せず実行される可能性があります。

■脆弱性がもたらす脅威

攻撃者がインストーラと同一フォルダに悪意のある DLL を配置した状態で、利用者が当該インストーラを実行した場合、その DLL が読み込まれ、悪意ある第三者によって任意のコードが実行される可能性があります。
これにより、以下のような被害が生じる恐れがあります。

- 不正プログラムのインストール
- データの改ざん・削除
- システムの不正操作

■対策方法

本脆弱性を解消した修正済みインストーラを公開しています。旧バージョン(Ver.1.0.0.0)のインストーラをお持ちのお客様は、旧バージョンを削除してから新インストーラ(Ver.2.0.0.0)をダウンロードしてください。

製品名称　　：LiveOnMeet クライアントインストーラ
対象アプリケーション：Downloader5Installer.exe
　　Downloader5InstallerForAdmin.exe
該当バージョン　　：Ver.2.0.0.0
ダウンロード URL　　：https://web.liveon.ne.jp/support/download/
ダウンロードファイル：Downloader5Installer_v2.zip
　　Downloader5InstallerForAdmin_v2.zip

製品名称　　：キヤノンネットワークカメラ用プラグインインストーラ
対象アプリケーション：CanonNWCamPlugin.exe
　　CanonNWCamPluginForAdmin.exe
該当バージョン　　：Ver.2.0.0.0
ダウンロード URL　　：https://web.liveon.ne.jp/support/download/

ダウンロードファイル：CanonNWCamPlugin_v2.zip
CanonNWCamPluginForAdmin_v2.zip

■回避策

修正済みインストーラへの更新が困難な場合、以下の回避策を実施することで本脆弱性の影響を緩和できます。

- インストーラの実行前に、インストーラと同一フォルダに不審な DLL ファイルが存在しないことを確認する。
- インストーラは、信頼できる場所（例：自身で作成した専用フォルダ）に単独で配置したうえで実行する。
- ダウンロードフォルダなど、第三者がファイルを配置できる可能性のあるフォルダでの実行を避ける。

※上記の回避策は脆弱性を根本的に解消するものではありません。可能な限り修正済みインストーラ（Ver.2.0.0.0）への更新を推奨します

■オンプレミス版をご利用のお客様へ

現在までにオンプレミス版で提供しているインストーラ(Ver.1.0.0.0)にも脆弱性は存在します。ただし、インストーラ実行時に同一フォルダに悪意のある DLL が存在しない限りは問題になることはありません。

インストーラの実行が必要な場合は可能な限り修正済みバージョン(Ver.2.0.0.0)での実行をお願いします（上記「対策方法」を参照ください)。修正済みバージョンの入手が難しい場合は、上記「回避策」を参照のうえ、インストール完了次第、旧インストーラ(Ver.1.0.0.0)の削除をお願いします。

■関連情報

JVN#45563482
LiveOn Meet の Windows PC用クライアントインストーラおよびプラグインインストーラにおける任意の DLL 読み込みの脆弱性

【 JVN(2026/4/22 公開)からの公表内容 】
日：https://jvn.jp/jp/JVN45563482/
英：https://jvn.jp/en/jp/JVN45563482/

■謝辞

本脆弱性をご報告いただき、JPCERT/CC を通じて本件をご連絡くださいました GMO サイバーセキュリティ by イエラエ株式会社 松本 一真 氏に深く感謝申し上げます。

■更新履歴

2026.04.21 この脆弱性情報ページを公開しました

■連絡先

本脆弱性対策情報に関するお問い合わせは、以下の窓口までご連絡ください。

ジャパンメディアシステム株式会社 脆弱性対応窓口
メール　：liveon-support@liveon.ne.jp
電話　　：03-5297-5511（平日 10:00～17:00）