

お客様各位

株式会社 アイ・ユー・ケイ
〒113-0024 東京都文京区西片 1-17-8 KS ビル
Tel : 03-5844-6035

MoonWalker V3 の DCOM 脆弱性対策 (CVE-2021-26414) について

拝啓

平素より、弊社製品に格別のご愛顧を賜り、誠にありがとうございます。

さて、この度 Microsoft 社から発表されておりました DCOM 脆弱性対策 (CVE-2021-26414) について、弊社製品 (MoonWalker V3) への影響が大きく至急の対策が必要となりますのでご案内申し上げます。

敬具

記

【事象について】

2022 年の第二四半期までに実施予定の Windows のアップデート (※1 参照) を適応した Windows 装置に対し、MoonWalker V3 の WMI を利用した監視 (監視指標、Windows イベントログ監視、プロセス監視) が行えなくなります。

なお、2021 年 11 月 1 日時点の Windows のアップデートを適応した Windows 装置では、イベントログにエラーメッセージ (ソース: DistributedCOM、イベント ID: 10036) が定期的に出力されますが、Windows 仕様変更への経過措置期間であるため 2022 年のアップデートが適用されるまでは MoonWalker V3 での監視自体は正常に動作します。

※1: Microsoft 社の該当情報 (2021 年 11 月 1 日時点)

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26414>

【MoonWalker V3 の対応について】

Windows の新しい仕様に対応した MoonWalker V3 のパッチを提供いたします。可能な限り早期に適用してください。なお、適用には以下の対応が必要となります。

(ア) MoonWalker V3.5.1 へのアップグレード

(イ) MoonWalker V3.5.1 への patch8 の適用 (2021 年 11 月 5 日リリース)

※ patch8 を適用後は監視を継続できますが、Windows 装置ではイベントログにエラーメッセージ (ソース: DistributedCOM、イベント ID: 10036) が引き続き出力される状況を確認しております。

このエラーメッセージの動作については今後の Microsoft 社の対応次第となります。

なお、メディア等が必要な場合はサポート窓口までご連絡をお願いします。

【MoonWalker V3.5.1 patch8 適応までの回避策について】

2021 年 12 月 31 日までに MoonWalker V3 のパッチ(patch8)適用が間に合わない場合、ご利用中の MoonWalker で監視を行うためには下記の対応が必要となります。

- ① 2021 年 12 月 31 日までを目途としてエージェントを使用した監視に切り替えることをご検討ください。
- ② 2022 年第二四半期に実施予定の Windows アップデートまで(Windows 仕様変更への経過措置期間)
Microsoft 社のサイト(※2)をご確認いただき、2021 年 12 月 31 日までを目途としてレジストリ値を無効と設定(Windows の再起動が必要になります)してください。イベントログにエラーメッセージ(ソース:DistributedCOM、イベント ID:10036)が定期的に出力されますが、継続して MoonWalker V3 の監視は動作いたします。

※2:Microsoft 社の該当情報(2021 年 11 月 1 日時点)

「WINDOWS DCOM Server セキュリティ機能バイパスの変更を管理する (CVE-2021-26414)」

<https://support.microsoft.com/ja-jp/topic/kb5004442-windows-dcom-server-%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E6%A9%9F%E8%83%BD%E3%83%90%E3%82%A4%E3%83%91%E3%82%B9%E3%81%AE%E5%A4%89%E6%9B%B4%E3%82%92%E7%AE%A1%E7%90%86%E3%81%99%E3%82%8B-cve-2021-26414-f1400b52-c141-43d2-941e-37ed901c769c>

- ③ 2022 年第二四半期に実施予定の Windows アップデート以降
回避策②は適用できなくなりますので、この Windows アップデートまでには MoonWalker V3 への対応実施をお願いします。
推奨はできませんが、どうしても更新ができない場合は、Windows のアップデート(※1 参照)を Windows へ適用しない(アンインストールする)という方法もございます。Microsoft 社が提供される情報を確認し各環境におけるリスク判断を行ったうえで対応をご検討ください。

【その他】

MoonWalker V3 のサポート期限(EOL)は 2023 年 3 月 31 日となっております。

ライセンスをご購入済みのお客様はサポート無しの前提でサポート期間終了後も引き続きご利用いただくことは可能ですが、サポート終了以後も Microsoft 社の仕様変更により製品が影響を受け動作しなくなる可能性がございます。

弊社では新製品 (Monarch2) もリリースしておりますので、移行も含めご検討いただけますようお願いいたします。

ご不明な点や移行についてのご相談がございましたら、下記のお問い合わせにご連絡頂きますようお願い申し上げます。

今後とも引き続きご愛顧賜りますよう宜しくお願い申し上げます。

お問い合わせ：株式会社アイ・ユー・ケイ アプリケーションソリューション本部 CST サービス部
e-mail:support@cloud-scope.com Tel: 03-5844-6035

以上