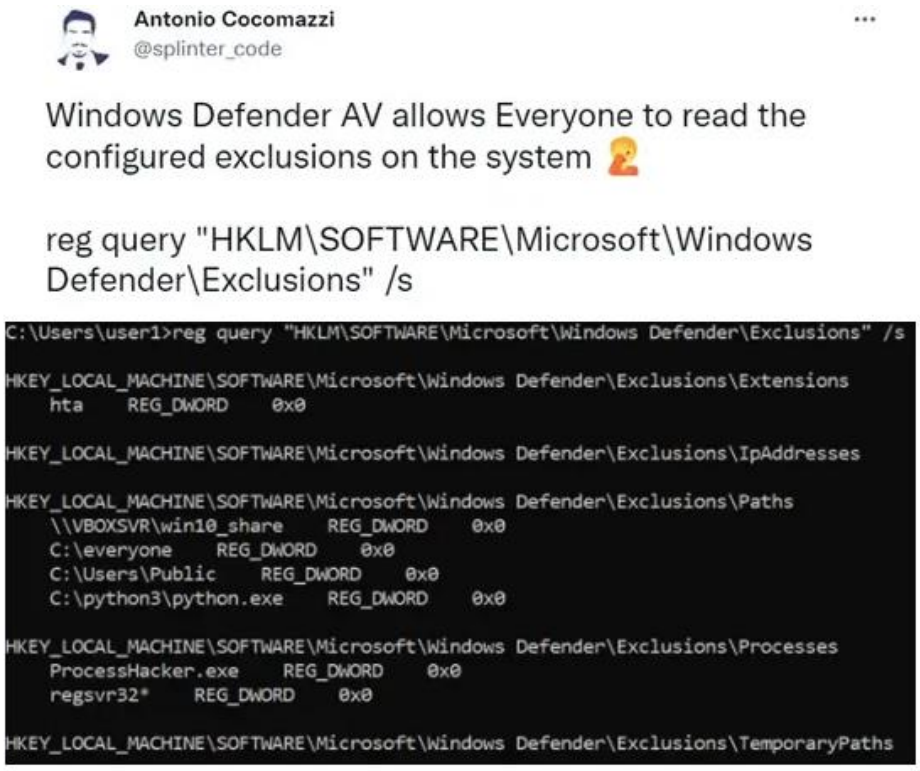
Windows Defender 脆弱性 — アンチウィルススキャン除外情報を読むことが可能に
2022 年 1 月 14 日 Minerva のブログから

Antonio Cocomazzi 氏のツイートによると“Windows Defender アンチウィルススキャン除外設定情報が誰でも(非管理者)閲覧可能になってしまうなどの重要なセキュリティリスクの可能性があるとの見解を示しました。



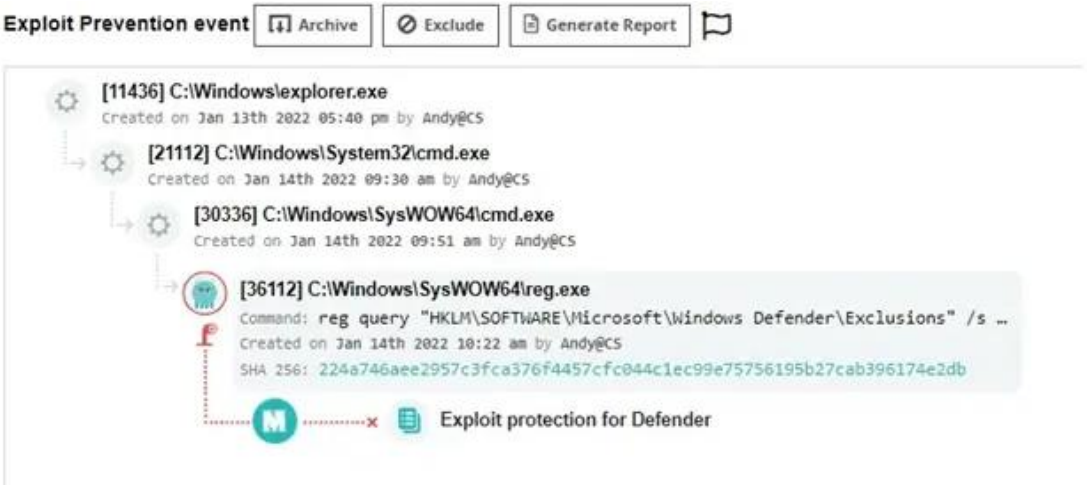
NathanMcNulty 氏はポリシーの設定でアンチウィルススキャン除外リストをコントロールすることが可能とツイートしています。
Reg query
“HLKM¥SOFTWARE¥Policies¥Microsoft¥Windows Defender¥Exclusions” /s

レポートによるとこの脆弱性は Windows11 ユーザーには影響しないようですが、Windows10 には脆弱性があります(Windows 10 バージョン 21H1 と 21H2 は要注意です)。

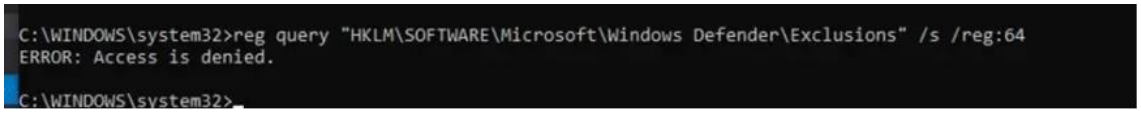
この脆弱性は reg コマンドがレジストリからアンチウィルススキャン除外情報を効果的に抜き出すことが可能になりセキュリティに影響を及ぼします。アンチウィルスに関する情報はとてもセンシティブかつ重要な機密情報です。この脆弱性で最も懸念する点は、誰でもアンチウィルススキャン除外設定の全貌をクエリーすることが可能になり、悪意のあるエクスプロイトがスキャン除外ホールダ/ファイル内へ埋め込むなどのセキュリティリスクが生じます。

さらに詳しい情報は Bleeping Computer の調査内容を参照ください。

Minerva 社提供の仮想パッチを当てることで脆弱性から守る
Minerva の仮想パッチでベンダーからの公式パッチリリースを待つことなく非管理者のクエリーからスキャン除外リストのレジストリへアクセスされず保護することができます。



Minerva 仮想パッチを実行することにより、エクスプロイト攻撃防御モジュールがクエリーをブロックします。



ユーザーがスキャン除外リストをクエリーしようとすると、アクセス拒否のエラーが返されます。

まとめ

Windows Defender のスキャン除外情報が読み取られると、攻撃を仕掛けられても無防備状態に陥るにも関わらず、Minerva の仮想パッチを利用する事によって企業組織のエンドポイントを容易に防御することが可能です。

Minerva 製品(Minerva Armor)についてのお問い合わせは Pico Technologies (info@pico-t.co.jp)までお願い致します。