ZJMR171211101

報道関係者各位

ニュースリリース

2017 年 12 月 11 日

ゾーホージャパン株式会社

ManageEngine の Active Directory 監査ソフト

JPCERT/CC 推奨のイベントログ監査に対応

Microsoft 公開の「Best Practices for Securing Active Directory」にも有効

ゾーホージャパン株式会社（代表取締役：迫 洋一郎、本社：横浜市、以下、ゾーホージャパン）は、Active Directory のログ監視および監査レポート作成に特化したソフトウェア「ManageEngine ADAudit Plus （マネージエンジン エーディーオーディット・プラス、以下、ADAudit Plus）」の最新版「ビルド 5050」を、2017 年 12 月 11 日にリリースしました。最新版は、一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）が高度サイバー攻撃への対処において監査を推奨するイベントログを収集できる他、Microsoft 公開の「Best Practices for Securing Active Directory」の内、重要度「高」のイベントログ監査にも対応しています。

- Active Directory 監査レポートソフト「ADAudit Plus」Web サイト
  https://www.manageengine.jp/products/ADAudit_Plus/

- JPCERT/CC 推奨のイベントログ監査に対応！Microsoft 推奨のイベントログ監査にも役立つ「ADAudit Plus」
  https://www.manageengine.jp/products/ADAudit_Plus/jpcertcc-microsoft-best-practice-for-securing-ad.html

【概要】

標的型攻撃が横行する昨今、攻撃者によって Active Directory が狙われるケースが多発しています。2017 年 3 月、JPCERT/CC からも解説書（ログを活用した Active Directory に対する攻撃の検知と対策）が公開され、Active Directory のセキュリティ保護が推奨されています。

ManageEngine では、早くから当解説書に則り Active Directory のログ監査／ID 管理を適切に行えるソリューションを提案してきました。この度のリリースにより、従来は統合ログ管理ソフト「EventLog Analyzer」と併用して監査するように提唱していた以下のイベントログを、全て ADAudit Plus のみで収集し、分かり易い監査レポートとして出力したり、リアルタイムのアラート通知を設定したりする事が可能となりました。

イベント ID	説明
4698	スケジュールされたタスクの作成
1102	イベントログの消去
4624	ログインの成功
4625	ログインの失敗
4768	Kerberos 認証 （TGT 要求）
4769	Kerberos 認証 （ST 要求）
4776	NTLM 認証
4672	特権の割り当て

これにより、Active Directory 監査担当者の作業負荷が大幅に軽減され、組織の更なるセキュリティレベル向上も期待できます。

（参考情報）

- ログを活用した Active Directory に対する攻撃の検知と対策（JPCERT/CC）
  https://www.jpcert.or.jp/research/AD.html

- Active Directory のセキュリティ対策ソリューション（ManageEngine）
  https://www.manageengine.jp/solutions/active_directory_security/lp/

- 統合ログ管理ソフト「EventLog Analyzer」
  https://www.manageengine.jp/products/EventLog_Analyzer/

【Microsoft 推奨のイベントログ監査にも有効】

ADAudit Plus 最新版「ビルド 5050」は、Microsoft が公開している「Best Practices for Securing Active Directory」で監視が推奨されているイベントログの内、下記の重要度「高」にも対応しています。

イベント ID	説明
4618	監視されるセキュリティイベントパターンが発生しました。
4649	リプレイ攻撃が検出されました。構成が正しくないエラーのための無害な誤検知があります。

4719	システム監査ポリシーが変更されました。
4765	SID 履歴がアカウントに追加されました。
4766	SID の履歴をアカウントに追加できませんでした。
4794	ディレクトリサービス復元モードの設定が試行されました。
4897	役割の分離が有効になっています。
4964	特別なグループが新しいログオンに割り当てられています。
5124	セキュリティの設定は、OCSP レスポンダーサービスに更新されました。

JPCERT/CC の解説書に加え、上記で推奨されているイベントログを監査したい場合にも ADAudit Plus は有用です。

Active Directory の監査については、日本市場では未だ大きく注目される機会が少ない反面、グローバル市場では既に注目度が高く、ADAudit Plus の販売数は急成長しています。ManageEngine では、今後もコストバランスの良い製品を提供することで、日本企業のセキュリティレベル底上げに貢献します。

（参考情報）

・ Best Practices for Securing Active Directory（Microsoft）
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

ADAudit Plus の最新版「ビルド 5050」についてのその他の情報は、以下のページで確認できます。

・ 「ADAudit Plus」リリース情報／新機能の紹介
https://www.manageengine.jp/products/ADAudit_Plus/release-note.html

【ADAudit Plus の価格および評価版ダウンロード】

「ADAudit Plus」では、30 日間無料で全機能を利用でき、技術サポートも受けられる「評価版」を提供しています。評価版は、以下のリンクよりダウンロードできます。なお、「ADAudit Plus」の有料版ライセンス料金については、以下の価格ページで確認できます。

・ 「ADAudit Plus」の評価版ダウンロード
https://www.manageengine.jp/products/ADAudit_Plus/download.html#trial

・ 「ADAudit Plus」の価格情報ページ

https://www.manageengine.jp/products/ADAudit_Plus/pricing.html

ADAudit Plus について

ADAudit Plus は、Active Directory のログ監視および監査レポートの作成に特化した Web ベースのソフトウェアです。Active Directory が出力したログを視覚的に見やすいレポート形式で表示し、ログの分析/解析にかかる工数を削減します。監査に必要とされているレポート（200 種類以上）を瞬時に作成することができる他、アラートを設定することでセキュリティ・インシデントの即時検知にも役立ちます。

ManageEngine
ADAudit Plus
https://www.manageengine.jp/products/ADAudit_Plus/

ManageEngine について

ManageEngine は、ゾーホージャパン株式会社が提供するネットワークや IT サービス、セキュリティ、デスクトップ・ノート PC、ビジネスアプリケーションなどを管理する製品・サービス群です。

必要十分な機能に限定、かつ、直感的な操作が可能な画面設計により、短期間での導入が可能であり、その後の運用フェーズにおいても手間がかからず、よりシンプルな IT 運用管理を実現します。

また、中堅・中小企業でも導入しやすいリーズナブルな価格で、これまで大手 IT ベンダーが提供する複雑で高額なツールを利用していた企業や、ツールを自社開発していた組織にも採用されてきました。現在では、日本国内の一般企業、官公庁や自治体などへ、4,000 ライセンスを超える販売実績があり、安心して使える製品・サービスです。

最大で 29 言語に対応する製品・サービスは、北米、欧州をはじめ、南米、中東、アジアなど世界で 12 万社以上の企業や組織が導入し、企業・組織の IT 運用管理のシンプル化、グローバル化に貢献しています。

ManageEngine
https://www.manageengine.jp/

ゾーホージャパン株式会社について

ゾーホージャパン株式会社は、ワールドワイドで事業を展開する Zoho Corporation Pvt Ltd が開発/製造したネットワーク管理開発ツールや企業向け IT 運用管理ツール、企業向けクラウドサービスを日本市場に提供すると同時に関連するサポート、コンサルティングなども提供しています。

ネットワーク管理開発ツール「WebNMS」は、シスコシステムズ、エリクソン、アルカテル・ルーセント、モト

ローラなど世界 2 万 5 千社の有力企業で採用され、ネットワーク管理の OEM 市場でデファクト・スタンダードとして認知されています。

　また、WebNMS のノウハウや経験を生かして開発された企業向け IT 運用管理ツール群「ManageEngine」は、世界 12 万社を超える顧客実績を誇り、国内でも販売本数を伸ばしています。

　その他、業務改善/生産性向上を支援する企業向けクラウドサービス群「Zoho」は、世界で 2500 万人を超えるユーザーに利用されています。

http://www.zoho.co.jp/

お問い合わせ先

本ニュースリリースに関するお問い合わせ：
ゾーホージャパン株式会社　ManageEngine & WebNMS 事業部 マーケティングチーム
TEL： 045-319-4613　E-mail: jp-memarketing@zohocorp.com