文書番号：SND-SEC-MI-19-106-1
2019 年 12 月 10 日
日本電気株式会社
サイバーセキュリティ戦略本部

2020 年初頭の Windows の更新プログラムに関する SECUREMASTER 製品への影響について

概要

Microsoft 社から以下の通知が出ています。

https://msrc-blog.microsoft.com/2019/10/02/ldapbinding/
https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/ADV190023

上記によると、2020 年初頭(日付未確定)に提供される Windows の更新プログラムにより Active Directory(以降 AD と記載します) の LDAP 署名、および LDAP チャネルバインディング （LDAPS 利用時）を既定で有効化されるとの記載があります。

上記について SECUREMASTER 製品への影響と対処について記載します。

対象製品

SECUREMASTER/EnterpriseIdentityManager 全バージョン
SECUREMASTER/EnterpriseDirectoryServer 全バージョン
SECUREMASTER/EnterpriseAccessManager 全バージョン

影響

上記対象製品に関して、AD に接続できない、AD に連携できないなど、正常に動作しない問題が発生します。

対処・回避策

対処については下記「影響を受けるコンポーネント及び対処」以降に記載している内容に従って下さい。
ただし、**製品の修正物件の適用または製品の設定変更ができない場合には、AD サーバにおいて当該 Windows の更新プログラムの適用を延期頂くか、Windows の更新プログラムの適用後に、AD サーバにおいて以下のレジストリ設定を戻して頂く対処**をお願いいたします。

レジストリキー
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥NTDS¥Parameters¥LDAPServer Integrity
設定する値：1(無効に相当)

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥ldap¥ldapclientintegrity
設定する値：1(2 になっている場合に 1 に変更)

影響を受けるコンポーネント及び対処

SECUREMASTER/EnterpriseIdentityManager(以下 EIM と記載します)

影響を受けるコンポーネント	影響及び対処	製品修正物件
AD 連携オプション	EIM→AD の連携(AD Sync-F)に影響があります。AD→EIM(AD Sync-W)には影響はありません。AD Sync-F については修正物件の適用が必要です。	提供予定 下記「製品の修正物件の提供について」を参照して下さい。
監査オプション	WebAP の[AD ユーザ確認用申請書フォーム]に影響があります。修正物件の適用が必要です。	下記「製品の修正物件の提供について」を参照して下さい。
AD インポートオプション（ad2eidm, Ver8.2 のみ)	AD への接続を TLS で保護するように製品設定を変更することで対処可能です。設定項目 adUserSSL にて AD への TLS 通信及び keystorePath にて設定します。 詳細は製品マニュアル「EnterpriseIdentityManager 利用の手引 AD インポートオプション編」を参照して下さい。	提供なし (製品設定変更で対処可能なため)
eidmsync eidmcheck eidmidchk	AD への接続を TLS で保護するように製品設定を変更することで対処可能です。 対処の詳細は下記「補足情報 1」を参照して下さい。	提供なし (製品設定変更で対処可能なため)

SECUREMASTER/EnterpriseDirectoryServer (以下 EDS と記載します)

影響を受けるコンポーネント	影響及び対処	製品修正物件
AD Sync-F オプション	EDS→AD の連携(AD Sync-F)に影響があります。AD→EDS(AD Sync-W)には影響はありません。 AD Sync-F については修正物件の適用が必要です。	提供予定 下記「製品の修正物件の提供について」を参照して下さい
eds2adsync（AD Sync-F オプションに含まれる EDS-AD 同期コマンド)	AD への接続を TLS で保護するように製品設定を変更することで対処可能です。 対処の詳細は下記「補足情報 2」を参照して下さい。 なお、eds2adsync についてはビルトイン証明書を使用でき	提供なし (製品設定変更で対処可能なため)

	ません。	

SECUREMASTER/EnterpriseAccessManager (以下 EAM と記載します)

影響を受けるコンポーネント	影響及び対処	製品修正物件
AuthServer	* 統合 Windows 認証時にユーザ属性情報を AD から取得する機能 [影響を受けるケース] 以下の条件をすべて満たす場合 (1) 統合 Windows 認証を利用 (2) WINCONFIG の設定を有効にしている (3) WINCONFIG-UDBSSL の設定に「false」を設定している [対処] 下記「補足情報 3」を参照して下さい。 *認証に成功したユーザ ID が実際に AD に存在するか確認する機能(Ver8.0 以降のみ) [影響を受けるケース] ADUSRCHECK の設定が「true」または TABLETAUTH の設定が「true」で、 かつ WINCONFIG-UDBSSL の設定が「false」の場合 [対処] 下記「補足情報 3」を参照して下さい。	提供なし (製品設定変更で対処可能なため)
SMWebAPI	認証済のユーザ ID が実際に AD に存在するか確認する機能(Ver8.0 以降) [影響を受けるケース] 以下の条件をすべて満たす場合に影響を受けます。 (1) AD ユーザ確認 API(本人)を呼び出している (2) WINCONFIG-UDBSSL の設定に「false」を設定している [対処] 下記「補足情報 4」を参照して下さい。	提供なし (製品設定変更で対処可能なため)

※AuthServer の[影響を受けるケース]、[対処]に記載の設定項目については、以下のいずれかの設定ファイルに記載されています。

・sm_auth_conf.xml

・sm_auth_default.xml

・sm_common_conf.xml

※SMWebAPI の[影響を受けるケース]、[対処]に記載の設定項目については、以下のいずれかの設定ファイルに記載

されています。設定が無い場合は対処不要です。

・sm_webapi_conf.xml

・sm_common_conf.xml

製品の修正物件の提供について

EIM

- AD 連携オプション

Ver8.0/8.1/8.2　2019 年 12 月 26 日に公開予定です。

Ver5.1 以前　　未定です。

- 監査オプション

現時点でパッチのリリース予定はありません。

PP サポート契約を締結しているお客様に対しては影響ある場合個別に対応いたしますので、弊社 PP サポートにお問い合わせください。

EDS

- AD Sync-F オプション

Ver8.0/8.1/8.2　2019 年 12 月 26 日に公開予定です

Ver7.1 以前　　未定です。

補足情報 1 (EIM の eidmsync,eidmcheck,eidmidchk)

eidmsync

-ssl オプションを指定すると、EIM(EDS)および AD への検索、AD(AD Sync-F 経由)への更新を行う際の通信で TLS を利用します。

-ssl オプションに加え -ksf オプション、-zf オプションを指定する必要があります。

eidmcheck、eidmidchk

-ssl オプションを指定すると、EIM(EDS)および AD への検索を行う際の通信で TLS を利用します。

-ssl オプションに加え -ksf オプションを指定する必要があります。

上記サーバに TLS 通信するには、事前に以下の作業が必要です。

なお、eidmsync を利用しない場合は、AD Sync-F の設定は不要です。

* AD にサーバ証明書を設定しておく必要があります。AD の設定については Microsoft の Web サイトを参照ください。
* EDS にサーバ証明書を設定しておく必要があります。製品のビルトイン証明書を利用する場合は不要です。
  設定方法については、EDS 運用の手引「第 12 章 SSL 通信」を参照ください。
* AD Sync-F の TLS 機能有効化、サーバ証明書の設定が必要です。
  製品のビルトイン証明書を利用する場合はサーバ証明書の設定は不要です。
  設定方法については、EIM 利用の手引 AD 連携オプション編の「2.5 SSL 通信」を参照ください。

-ksf オプション

EIM(EDS)と AD の CA 証明書を格納したキーストアを指定します。

ビルトイン証明書を使用して TLS 通信する場合のキーストアの作成例は以下になります。

手順は EIM サーバで実施します。

1. ビルトイン証明書を任意のパスにコピーします。
   ビルトイン証明書のパスは以下になります。
   Linux 版 … /etc/opt/nec/eds/built-in-CA.pem
   Windows 版 … {Windows フォルダ}¥EDS¥built-in-CA.pem
2. コピーした証明書を編集します。
   証明書が 2 つ格納されているので、一つ目の
   「-----BEGIN CERTIFICATE----- ～ -----END CERTIFICATE-----」を
   削除します。
3. keytool コマンドでビルトイン証明書をキーストアにインポートします。
   Linux 版
   /usr/java/jdk/bin/keytool
   -import -alias cacerts-eim -file {2.で編集したファイル}
   -trustcacerts -keystore {キーストアのファイルパス}

-storepass {キーストアのパスワード} -storetype JKS

Windows 版

{EIM インストールパス}¥JRE¥bin¥keytool.exe

-import -alias cacerts-eim -file {2.で編集したファイル}

-trustcacerts -keystore {キーストアのファイルパス}

-storepass {キーストアのパスワード} -storetype JKS

※それぞれ 1 行のコマンドです

4. keytool コマンドで AD の CA 証明書をキーストアにインポートします。

Linux 版

/usr/java/jdk/bin/keytool

-import -alias cacerts-ad -file {AD の CA 証明書}

-trustcacerts -keystore {3.で指定したキーストアのパス}

-storepass {キーストアのパスワード} -storetype JKS

Windows 版

{EIM インストールパス}¥JRE¥bin¥keytool.exe

-import -alias cacerts-ad -file {AD の CA 証明書}

-trustcacerts -keystore {3.で指定したキーストアのパス}

-storepass {キーストアのパスワード} -storetype JKS

※それぞれ 1 行のコマンドです

-zf オプション

AD Sync-F の CA 証明書を利用する設定ファイルを指定します。

設定ファイルの詳細は EIM 利用の手引「10.5.1 eidmsync コマンド」の-zf オプションの説明を参照ください。

ビルトイン証明書を使用する場合の設定例は以下になります。

Linux 版

-zf /etc/opt/nec/eds/tls.conf

Windows 版

-zf C:¥Windows¥EDS¥tls.conf

補足情報 2 (EDS の eds2adsync)

eds2adsyncは、eds2adsync設定ファイルで sslオプションを指定すると、EDSおよびADへの検索、AD(AD Sync-F 経由)への更新を行う際の通信で TLS を利用します。

ssl オプションに加え EDScacert オプション、ADcacert オプション、ADFcacert オプションを指定する必要があります。

AD サーバに TLS 通信するには、事前に以下の作業が必要です。

* AD にサーバ証明書を設定しておく必要があります。AD の設定については Microsoft の Web サイトを参照ください。

* EDS にサーバ証明書を設定しておく必要があります。
  設定方法については、EDS 運用の手引「第 12 章 SSL 通信」を参照ください。
* AD Sync-F の TLS 機能有効化、サーバ証明書の設定が必要です。
  設定方法については、EIM 利用の手引 AD 連携オプション編の「2.5 SSL 通信」を参照ください。

EDScacert オプション、ADcacert オプション、ADFcacert オプションについて説明します。
* EDScacert オプションには EDS サーバ証明書を署名した CA の証明書のファイルパスを指定します。
* ADcacert オプションには AD サーバ証明書を署名した CA の証明書のファイルパスを指定します。
* ADFcacert オプションには AD Sync-F サーバ証明書を署名した CA の証明書のファイルパスを指定します。

補足情報 3 (EAM の AuthServer)

統合 Windows 認証時にユーザ属性情報を Active Directory から取得する機能についての対処
「統合 Windows 認証機能導入手順書」の「2.4 LDAPS の設定」に従い、AD の証明書をキーストアファイルに格納します。
合わせて、WINCONFIG-UDBSSLSTORE にて上記キーストアファイルの指定と、WINCONFIG-UDBPORT を AD の SSL 用ポート番号に変更、WINCONFIG-UDBSSL を「true」に設定します。

認証に成功したユーザ ID が実際に Active Directory に存在するか確認する機能についての対処
「統合 Windows 認証機能導入手順書」の「2.4 LDAPS の設定」に従い、Active Directory の証明書をキーストアファイルに格納します。
合わせて、WINCONFIG-UDBSSLSTORE にて上記キーストアファイルの指定と、WINCONFIG-UDBPORT を AD の SSL 用ポート番号に変更、WINCONFIG-UDBSSL を「true」に設定します。

補足情報 4 (EAM の SMWebAPI)

AuthServer の「統合 Windows 認証機能導入手順書」の「2.4 LDAPS の設定」に従い、AD の証明書をキーストアファイルに格納します。
合わせて、WINCONFIG-UDBSSLSTORE にて上記キーストアファイルの指定と、WINCONFIG-UDBPORT を AD の SSL 用ポート番号に変更、WINCONFIG-UDBSSL を「true」に設定します。

以上