

「OpenSSL の脆弱性」のマジックコネク トへの影響

作成:2014 年 4 月

更新:2017 年 4 月

NTT テクノクロス株式会社

JPCERT/CC など各セキュリティ対策機関より注意喚起が行われている、OpenSSL の heartbeat 拡張に関する脆弱性 (CVE-2014-0160, <https://www.jpcert.or.jp/at/2014/at140013.html>) について、マジックコネク トへの影響範囲、影響を受ける場合の対策をご案内します。

- マジックコネク トサーバは本脆弱性の影響を受けません。(本脆弱性が存在するバージョンの OpenSSL は、過去を含めて利用していません。)
- マジックコネク トのビューア、クライアントの一部プログラムは、本脆弱性の影響を受ける可能性があります。

下記のいずれかに該当するお客様は、本脆弱性の影響を受ける可能性があります。

該当する場合、お手数ですが後述の内容に従って、確認と対策の実施をお願いします。

- ◆ Android 版ビューアプログラムを利用している。
- ◆ サービス提供開始日(※)が、**2014 年 4 月 1 日から 4 月 18 日**の USB キー、指紋認証 USB キーを利用している。(※サービス提供開始日はユーザアカウント一覧に記載されています。)
- ◆ 弊社 Web サイトから、**2014 年 4 月 1 日から 4 月 15 日**の間にダウンロードしたビューア、クライアントプログラムを利用している。

いずれにも該当しない場合は、本脆弱性の影響を受けませんので対策は不要です。

影響と対策

本脆弱性の影響を受けるプログラムをご利用の場合、偽装された不正なサーバに誘導され接続すると、悪意の第三者にマジックコネクットの認証情報が漏洩する可能性があります。

ただし、マジックコネクットは多要素認証を採用しています。そのため、認証情報が漏洩しても、USB キーや登録された端末が盗まれない限りマジックコネクットが不正に利用されることはありません。

リスクを最小化するため、該当するプログラムをご利用のお客様は、

- ◆ 対処済みバージョンへアップデートの後、
- ◆ マジックコネクットのパスワードを変更してください。

マジックコネクットのパスワードは、管理機能を利用して変更することができます。

<http://www.magicconnect.net/support/tool/support-access.php>

該当するプログラムの具体的な情報と、アップデート方法を以下にご案内します。

記載されているバージョンより古いバージョン、及び 新しいバージョンは本脆弱性の影響を受けないため、アップデート対象外です。対策を実施していただく必要はありません。

※ ビュープログラムは「操作をする側（手元端末）のプログラム」を指します。

※ クライアントプログラムは「操作をされる側（対象機器）のプログラム」を指します。

- サービス提供開始日が、2014年4月1日から4月18日の【USB型・指紋認証型】のビュープログラム

バージョン: 4.2r1

- 該当するバージョンを出荷したアカウント管理者様へ、アップデート方法を別途連絡させていただきます。

- 弊社Webサイトから、2014年4月1日から4月15日の間にダウンロードした【クライアント】プログラム

バージョン: 3.3r4

- 最新のバージョン 3.3r5 へアップデートしてください。バージョンの確認方法を含むアップデートの手順は下記のページをご参照ください。

- 最新クライアントへのバージョンアップ手順

http://www.magicconnect.net/support/manual/mcclient_update.php

- 最新クライアントへのバージョンアップ手順(モバイル用)

http://www.magicconnect.net/support/manual/mcclient_mobile_update.php

- Google Play ストアから、2013 年 5 月から 2014 年 4 月 14 日の間にダウンロードした【Android】版ビューアプログラム

バージョン: 3.9r1 及び 4.1r3

- バージョンの確認方法は本文書末尾の「別紙」をご参照ください。
- 該当するバージョンの場合、Google Play ストアより最新のバージョン 4.1r4 へアップデートしてください。
 - ☆ Android 版ビューアプログラムに会社 PC の Windows ログオンパスワードを保存していた場合、マジックコネクトのパスワードに加え、会社 PC の Windows ログオンパスワードも変更してください。

- 弊社 Web サイトから、2014 年 4 月 1 日から 4 月 15 日の間にダウンロードした【端末認証型】のビューアプログラム

バージョン: 4.2r1

- バージョンの確認方法は本文書末尾の「別紙」をご参照ください。
- 該当するバージョンの場合、下記のページより端末認証型のセットアップパッケージを再ダウンロードし、最新のバージョン 4.2r2 を上書きインストールしてください。

<http://www.magicconnect.net/download/setup.php>

以下のプログラムは、すべてのバージョンにおいて、本脆弱性の影響を受けません。

- ◆ マジックコネクトサーバ
- ◆ iOS 版ビューアプログラム
- ◆ DLO 型ビューアプログラム
- ◆ MC3000 クライアントプログラム

別紙：バージョンの確認方法

Android 版ビューアプログラム、端末認証型ビューアプログラム のバージョンの確認方法をご案内します。

A. Android 版ビューアプログラム



B. 端末認証型ビューアプログラム

