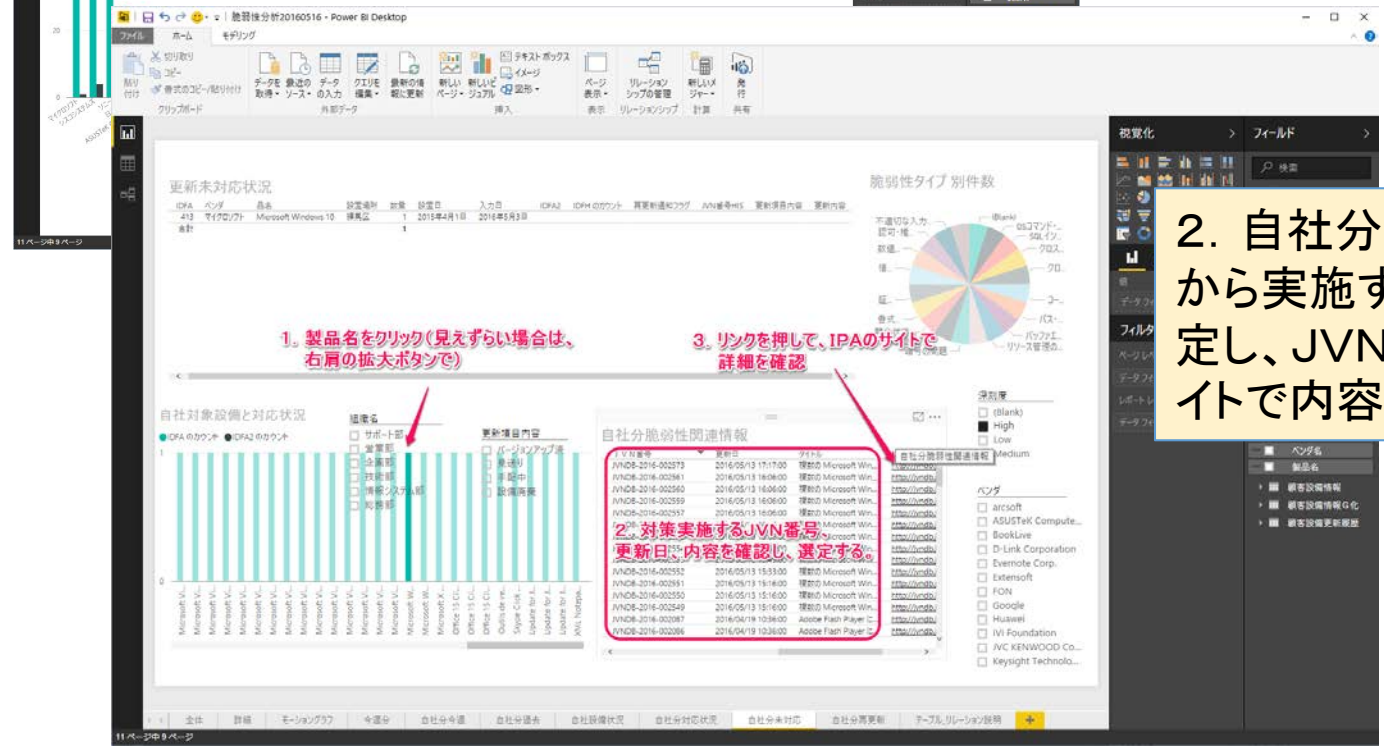


5. 脆弱性対策の策定方法 (1) PowerBIから対策の選定



1. 自社未対応のレポートからベンダ、品名を選択



2. 自社分脆弱性関連情報から実施するJVN番号を選定し、JVNの詳細リンクサイトで内容を確認する

5. 脆弱性対策の策定方法 (1) PowerBIから対策の選定

最終更新日: 2016/05/13

JVN iPedia 脆弱性対策情報データベース

JVNDB-2016-002573

複数の Microsoft Windows 製品の Windows Journal における任意のコードを実行される脆弱性

概要

複数の Microsoft Windows 製品の Windows Journal には、任意のコードを実行される脆弱性が存在します。

3. IPAサイトでJVNの詳細内容を確認

CVSS による深刻度 (CVSS とは?)

基本値: **9.3 (危険)** [NVD値]

- 攻撃元区分: ネットワーク
- 攻撃条件の複雑さ: 中
- 攻撃前の認証要素: 不要
- 機密性への影響(C): 全面的
- 完全性への影響(I): 全面的
- 可用性への影響(A): 全面的

[参考] CVSS v3 による深刻度
基本値: **7.8 (重要)** [NVD値]

- 攻撃元区分: ローカル
- 攻撃条件の複雑さ: 低
- 攻撃に必要な特権レベル: 不要
- 利用者の関与: 要
- 影響の想定範囲: 変更なし

IPAのサイトで対策を実施するか内容を確認して判断する

影響を受けるシステム

IPAのサイトでベンダの情報を確認する

マイクロソフト

- Microsoft Windows 10 for 32-bit Systems
- Microsoft Windows 10 for x64-based Systems
- Microsoft Windows 10 Version 1511 for 32-bit Systems
- Microsoft Windows 10 Version 1511 for x64-based Systems
- Microsoft Windows 7 for 32-bit Systems SP1
- Microsoft Windows 7 for x64-based Systems SP1
- Microsoft Windows 8.1 for 32-bit Systems
- Microsoft Windows 8.1 for x64-based Systems
- Microsoft Windows RT 8.1
- Microsoft Windows Vista SP2
- Microsoft Windows Vista x64 Edition SP2

想定される影響

第三者により、巧妙に悪用される可能性があります。

対策

4. ベンダの詳細内容をさらに確認する

ベンダより正式な対策が公開されています。ベンダ情報を参照して適切な対策を実施してください。

ベンダ情報

ベンダのサイトでさらに詳細を確認

マイクロソフト

- Microsoft Security Bulletin : **MS16-056**
- マイクロソフト セキュリティ情報 : **MS16-056**

CWEによる脆弱性タイプ一覧 CWEとは?

5. 脆弱性対策の策定方法 (1) PowerBIから対策の選定

Microsoft | TechNet
日本 (日本語) サインイン

セキュリティ TechCenter
検索

ホーム セキュリティ更新プログラム ツール ライブラリ ラーニング

5. ベンダのバージョンアップのプログラムを確認し、対策を計画する

- ▶ セキュリティ アドバイザリとセキュリティ情報
- ▶ セキュリティ情報
- 2016
 - [MS16-067](#)
 - [MS16-066](#)
 - [MS16-065](#)
 - [MS16-064](#)
 - [MS16-062](#)
 - [MS16-061](#)
 - [MS16-060](#)
 - [MS16-059](#)
 - [MS16-058](#)
 - [MS16-057](#)
 - MS16-056**
 - [MS16-055](#)
 - [MS16-054](#)
 - [MS16-053](#)
 - [MS16-052](#)
 - [MS16-051](#)
 - [MS16-050](#)
 - [MS16-049](#)
 - [MS16-048](#)
 - [MS16-047](#)
 - [MS16-046](#)
 - [MS16-045](#)

マイクロソフト セキュリティ情報 MS16-056 - 緊急

Windows Journal 用のセキュリティ更新プログラム (3156761)

公開日: 2016 年 5 月 11 日

バージョン: 1.0

ベンダサイトでバージョンアップのプログラムを確認し、対策の実施を計画する

▲ 概要

このセキュリティ更新プログラムは、Microsoft Windows の脆弱性を解決します。この脆弱性で、特別に細工されたジャーナル ファイルをユーザーが開いた場合にリモートでコードが実行される可能性があります。コンピューターでのユーザー権限が低い設定のアカウントを持つユーザーは、管理者特権で実行しているユーザーよりもこの脆弱性による影響が少ないと考えられます。

このセキュリティ更新プログラムは、すべてのサポートされているエディションの Windows Vista、Windows 7、Windows 8.1、Windows RT 8.1、および Windows 10 について、深刻度が「緊急」と評価されています。詳細については、「影響を受けるソフトウェア」のセクションを参照してください。

このセキュリティ更新プログラムは Windows Journal がジャーナル ファイルを解析する方法を変更することにより、この脆弱性を解決します。脆弱性の詳細については、「脆弱性の情報」を参照してください。

この更新プログラムの詳細については、[マイクロソフト サポート技術情報 3156761](#) を参照してください。

▲ 影響を受けるソフトウェアと脅威の深刻度

次のソフトウェア バージョンまたはエディションが影響を受けます。一覧にないバージョンまたはエディションは、サポート ライフサイクルが終了しているか、この脆弱性の影響を

このページのトピック:

- [概要](#)
- [影響を受けるソフトウェアと脅威の深刻度](#)
- [脆弱性の情報](#)
- [セキュリティ更新プログラムの展開](#)
- [謝辞](#)
- [免責](#)
- [更新履歴](#)

すべて折りたたむ
エクスポート (0)
印刷

5. 脆弱性対策の策定方法

(2) 顧客設備更新履歴に入力

- 更新する顧客設備情報のIDFAを顧客設備更新履歴のIDFA2に入力します。
- 選択したJVN番号をJVN番号HISに入力します。
- 更新項目内容は、プルダウンで選択してください。
- 更新日、更新内容(オプション)を入力します。
- 作成した顧客設備更新履歴のエクセルをPowerBIに読み込ませて完了です。情報が反映されていることを確認してください。

IDFH	IDFA2	顧客ID HIS	JVN番号HIS	更新項目 id	更新項目内容	更新日	更新内容	再更新通知 フラグ	削除フラグ
1	1 T0026		JVNDB-2014-005239	1	バージョンアップ済	2016/01/02	ファームバージョンアップする	1	

5. 脆弱性対策の策定方法 (2) 顧客設備更新履歴に入力の裏技

データエクスポートできます。
CSVで出力されますが、
文字化けするので、拡張子
をtxtにして開きます。

JVNB番号をコピーして使ってください

IDFA2	IDFA	ベンダ	品名	深刻度	JVN番号	更新日	タイム	内容
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002573	2016-05-13 17:17:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する Windows Journal の脆弱性に関する CVE-2016-002573
.1.1	.1	マイクロソフト	Microsoft Windows	Low	JVNB-2016-002571	2016-05-13 16:59:00	Microsoft	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002571
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002561	2016-05-13 16:06:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002561
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002560	2016-05-13 16:06:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002560
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002559	2016-05-13 16:06:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002559
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002558	2016-05-13 16:06:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002558
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002557	2016-05-13 16:06:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002557
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002556	2016-05-13 16:06:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002556
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002555	2016-05-13 15:59:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002555
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002554	2016-05-13 15:49:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002554
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002549	2016-05-13 15:16:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002549
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002548	2016-05-13 15:16:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002548
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002547	2016-05-13 15:16:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002547
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002087	2016-04-19 10:36:00	Adobe Fla	Adobe Flash Player には、有名な CVE-2016-002087 の脆弱性に関する CVE-2016-002087
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002046	2016-04-15 12:17:00	Microsoft	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002046
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002045	2016-04-15 12:17:00	Microsoft	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002045
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002044	2016-04-15 12:17:00	Microsoft	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002044
.1.1	.1	マイクロソフト	Microsoft Windows	Low	JVNB-2016-002043	2016-04-15 12:16:00	複数の Mic	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002043
.1.1	.1	マイクロソフト	Microsoft Windows	Low	JVNB-2016-002042	2016-04-15 12:16:00	複数の Mic	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002042
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002041	2016-04-15 12:16:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002041
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002023	2016-04-15 11:41:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002023
.1.1	.1	マイクロソフト	Microsoft Windows	High	JVNB-2016-002022	2016-04-15 11:41:00	複数の Mi	複数の Microsoft Windows 10 の脆弱性に関する CVE-2016-002022

1. 自社分関連脆弱性情報のレポートの右肩をクリックしてデータをエクスポートします。CSVで出力されますが、文字化けするので、拡張子をtxtで開いてください

2. 開いたtxtファイルから該当のJVNB番号をコピーして更新履歴のJVNB番号HISに入力してください。