セキュリティ情報収集・活用訓練
座学資料

訓練概要

- 訓練目的
  - iDefense セキュリティインテリジェンスサービスを利用して下記のセキュリティ情報を収集し、セキュリティ対策や分析に活用できる様にする。

    〇 脆弱性情報（オペレーションシステムやソフトウェア、ファームウェアなど）
    〇 脅威情報（ハクティビスト、ゼロデイ、マルウェアの動向など）
- 受講対象
  - 新規隊員
  - セキュリティ管理・運用者、ネットワーク運用・管理者
  - マルウェアや攻撃手法の動向などの分析調査・研究を行う者
  - 国内外の脅威情報を収集し、予防処置や事前対策の立案を行う者
- 受講可能レベル
  - 下記事前知識を有する者
- 事前知識
  - 基本的なセキュリティ用語（脆弱性，脅威，CVE，CVSS 等）
  - 基本的なネットワークの知識（IPアドレス，ポート，サービス，プロトコル等）

目次

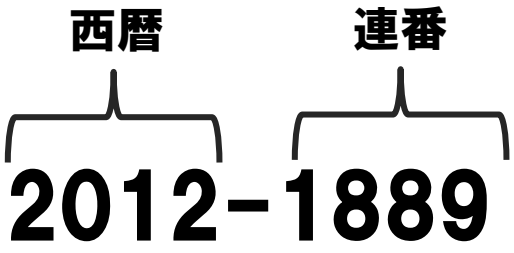
- 座学（40分）
  - 脆弱性に関わる一般技術概要
  - 脆弱性に関わる情報源
  - ソフトウェアのバージョン確認方法
  - 脆弱性の調査方法
- 演習（20分）
  - 脆弱性の調査

脆弱性に関わる一般技術概要

- CVE（Common Vulnerabilities and Exposures）
- CVSS（Common Vulnerability Scoring System）
- PoC（Proof-of-Concept）
- セキュリティ修正パッチ
- ゼロデイ攻撃
- ハクティビスト

CVE(Common Vulnerabilities and Exposures)

- 共通脆弱性識別子
- プログラムに存在する脆弱性に対して、一意に付与される識別子

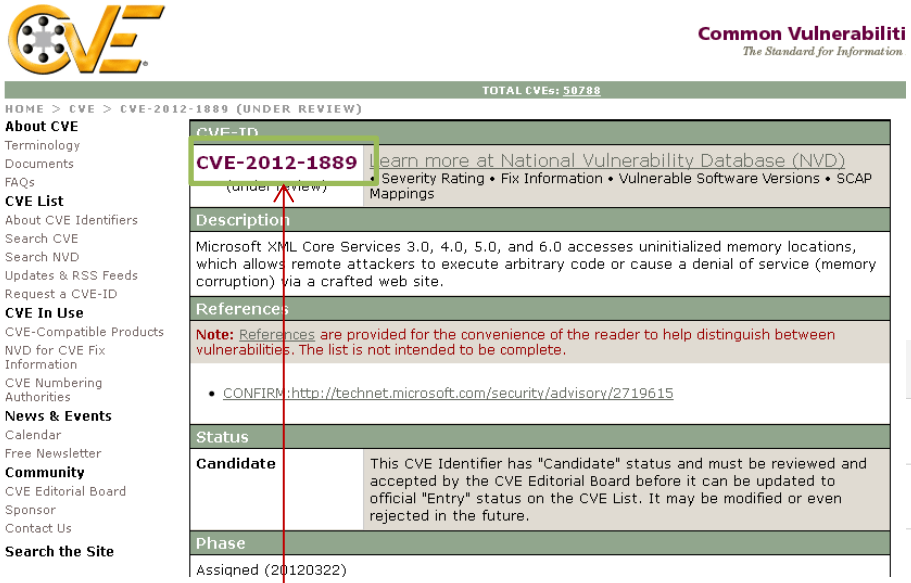


  - 脆弱性対策情報の参照番号としての利用
  - 異なる組織から公開されている脆弱性対策情報同士の関連付けに利用

  - 関連付けの例

MS012-043 ↔ CVE-2012-1889 ↔ JVNTA12-174A

CVE(Common Vulnerabilities and Exposures)



Common Vulnerabiliti
The Standard for Information

TOTAL CVEs: 50788

HOME > CVE > CVE-2012-1889 (UNDER REVIEW)

About CVE
Terminology
Documents
FAQs
CVE List
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID
CVE In Use
CVE-Compatible Products
NVD for CVE Fix Information
CVE Numbering Authorities
News & Events
Calendar
Free Newsletter
Community
CVE Editorial Board
Sponsor
Contact Us
Search the Site

CVE-ID

CVE-2012-1889 (under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Microsoft XML Core Services 3.0, 4.0, 5.0, and 6.0 accesses uninitialized memory locations, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:http://technet.microsoft.com/security/advisory/2719615

Status

Candidate

This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

Phase

Assigned (20120322)

CVE番号を確認することで、
同じソフトウェアの
脆弱性情報と判断可能

JVNTA12-174A
Microsoft XML コアサービスに脆弱性

概要
Microsoft XML コアサービスには、任意のコードが実行される脆弱性が存在します。

影響を受けるシステム
対象となる製品は複数存在します。詳しくは Microsoft が提供する情報をご確認ください。

詳細情報
Microsoft Office 2003、2007 や Internet Explorer などで使用されている Microsoft XML コアサービスには、データの処理に問題があり、任意のコードが実行される脆弱性が存在します。

Microsoft によると、本脆弱性を使用した攻撃が観測されているとのことです。

想定される影響
細工されたウェブページや Office ドキュメントを開くことで、ユーザの権限で任意のコードが実行される可能性があります。

関連文書

JPCERT 緊急報告	JPCERT-AT-2012-0020 2012年6月 Microsoft セキュリティ情報 (緊急 3件含) に関する注意喚起
JPCERT REPORT	
CERT Advisory	US-CERT Alert (TA12-174A) Microsoft XML Core Services Attack Activity
CPNI Advisory	
TRnotes	
CVE	CVE-2012-1889
JVN iPedia	

CVEの活用

- CVE で検索してみると、様々な組織が提供している同じ脆弱性に関する情報が得られる。

CVEの活用例

Aさん：Adobe Flash Player　の任意のコード実行の脆弱性
の影響を受けるバージョンを教えてください。

Bさん：えっ！たくさんあるけど、どれだろう・・・
(CVE-2012-5272、CVE-2011-2416 etc。。。)

Aさん：Adobe Flash Player　の任意のコード実行の脆弱性
CVE-2012-5272 の件についてですが・・・・

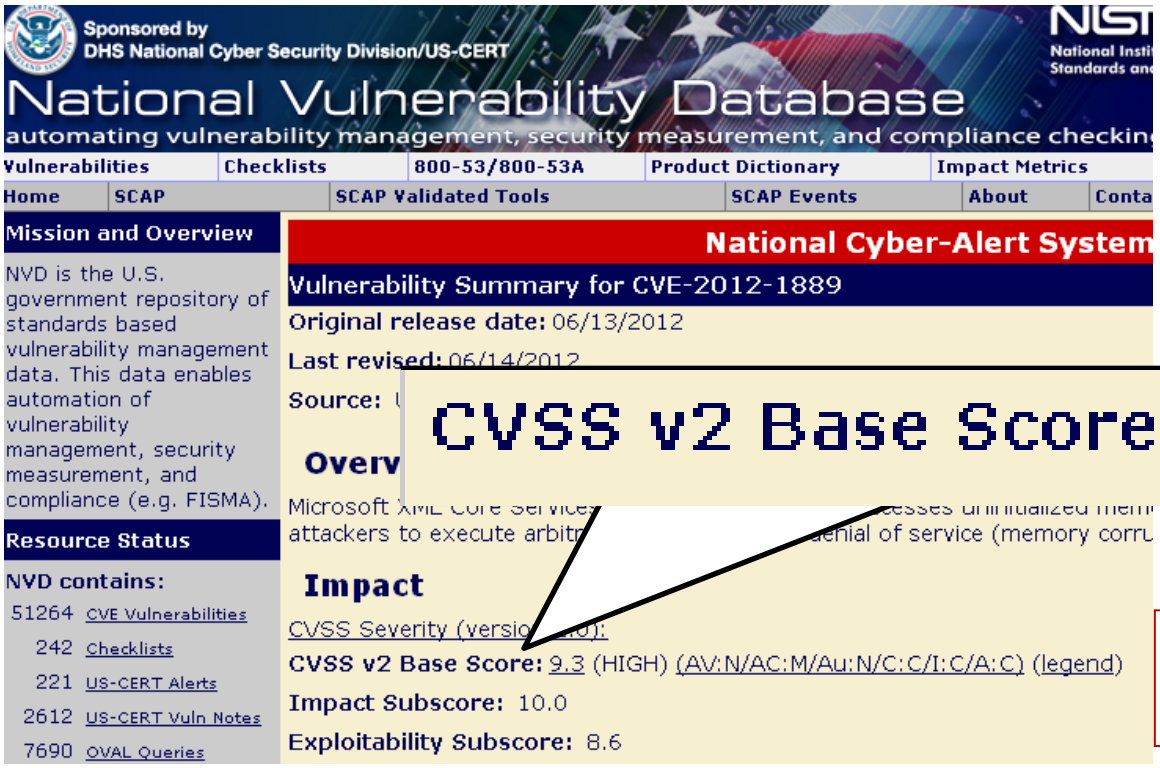
Bさん：CVE-2012-5272 についてですね。
Adobe Flash Player 10.3.181.34およびそれ以前他・・・

CVSS(Common Vulnerability Scoring System)

- 共通脆弱性評価システム
- 情報システムの脆弱性に対するオープンで汎用的な評価手法
- 脆弱性自体の特性＜基本評価基準＞、パッチの提供状況＜現状評価基準＞、ユーザ環境＜環境評価基準＞での影響度などを考慮し影響度を評価する。

CVSS(Common Vulnerability Scoring System)

- CVE-2012-1889



深刻度	基本値
I（High）	7.0~10.0
II（Middle）	4.0～6.9
III（Low）	0.0～3.9

脆弱性の深刻度を判断可能

0 ——— 10.0

9.3

CVSS の活用例

Aさん：使っているシステムに、CVE-2011-3607(Apache)と
CVE-2012-2376(PHP)の脆弱性があるので、
なるべく早く対応して。

Bさん：アップデートするには、検証が必要だから時間がかかる。
検証が終わったものから順次対応したいけど、
どちらからやれば良いだろう・・・

Aさん：使っているシステムに、CVE-2011-3607(Apache)と
CVE-2012-2376(PHP)の脆弱性があるので、
なるべく早く対応して。

Bさん：CVE-2011-3607(Apache)の CVSS　は、4.4。
CVE-2012-2376(PHP)の CVSS は、10.0。
CVE-2012-2376(PHP)の検証から始めよう！

PoC（Proof-of-Concept）

- 脆弱性を悪用した攻撃が実際に有効であることを検証するためのプログラム
- PoC　≒　エクスプロイトコード
- コードを改造することで、攻撃プログラムになりうる
- 脆弱性の対応策が確立する前にPoCが公開されると危険な状態となる

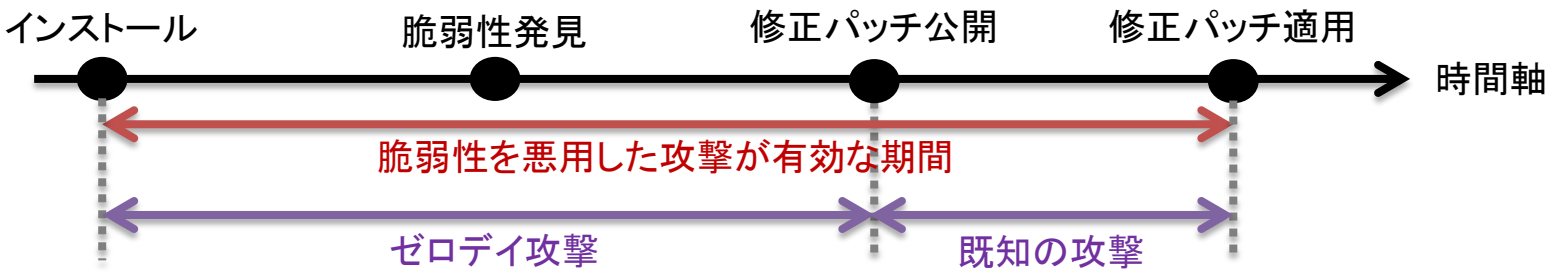
セキュリティ修正パッチ

- 脆弱性を排除するために、ソフトウェアのベンダがユーザに提供する修正プログラム

- 脆弱性を悪用した不正アクセスは、インストールされているソフトウェアの脆弱性を排除することで予防できる
- 既知の脆弱性は、対象ソフトウェアのベンダが提供するセキュリティ修正パッチの適用により排除できる

ゼロデイ攻撃

- セキュリティ修正パッチが公開される前の脆弱性を悪用した攻撃
- そのため、最新版のソフトウェアに対しても攻撃が有効となる



ハクティビスト

- ハクティビストとは
  - 社会的・政治的な主張を目的としたハッキング活動（ハクティビズム）を行う者
  - ハッカー（hacker）と活動家（activist）を組み合わせた造語
  - 「アノニマス（Anonymous）」が有名
- 主な攻撃事例
  - #OpSony (2011年4月)
    - PS3のハッキング問題に関連したDDoS攻撃
  - #OpJapan (2012年7月)
    - 日本の著作権法の改正に関連したDDoS攻撃、Web改ざん

脆弱性に関わる情報源

- ベンダ情報
- NVD（National Vulnerability Database）
- JVN（Japan Vulnerability Notes）
- iDefenseセキュリティインテリジェンスサービス

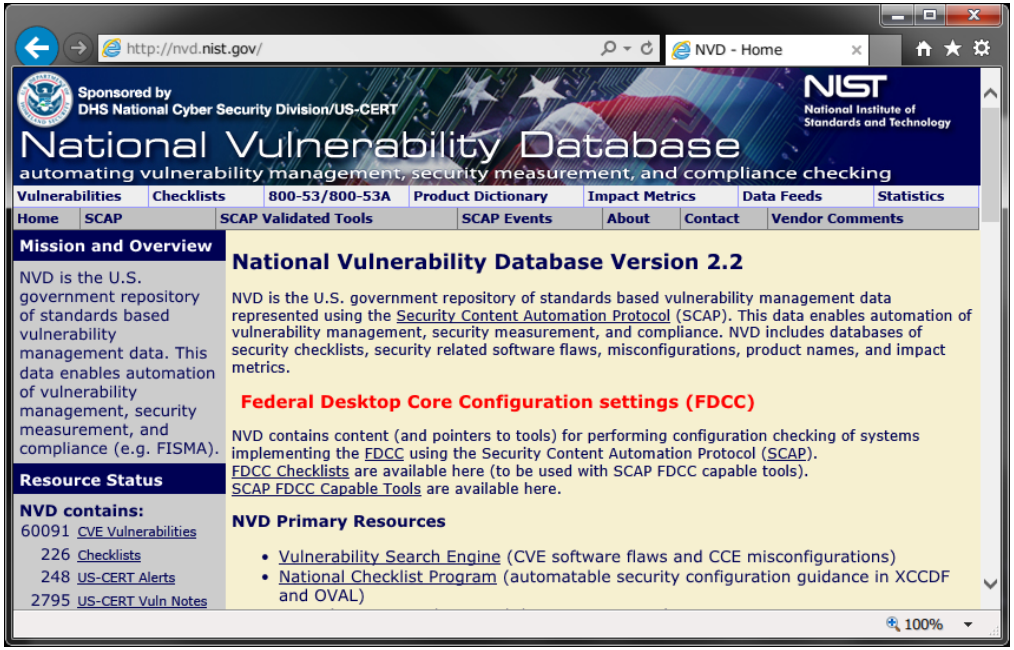
ベンダ情報

- ソフトウェアの開発元が提供する情報
  - 脆弱性の概要、影響するバージョン、対策情報など
- 脆弱性情報の中でも信頼度が高い

Microsoftの製品の脆弱性に関する情報の例

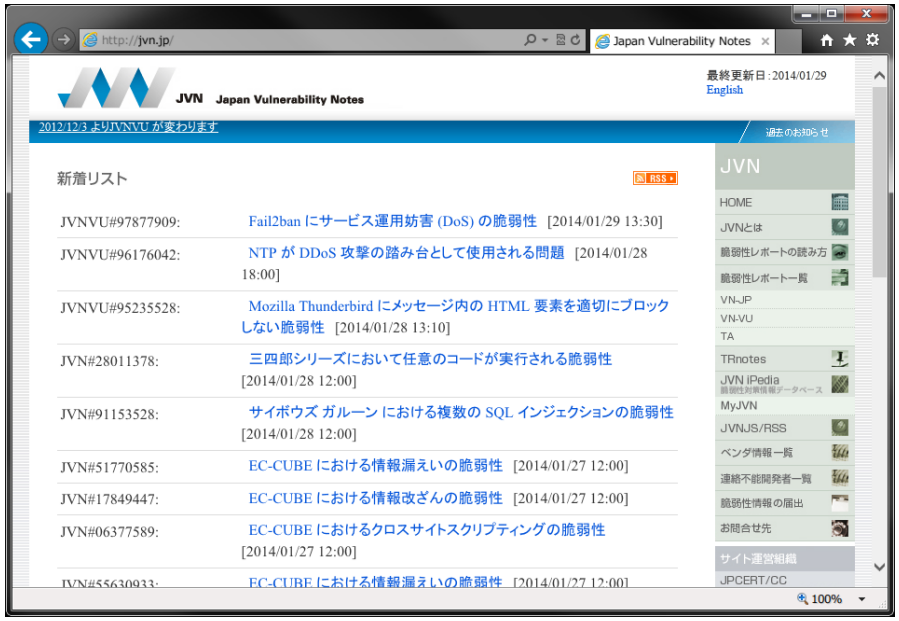
NVD（National Vulnerability Database）

- NIST（米国国立標準技術研究所）が管理する脆弱性情報データベース



JVN（Japan Vulnerability Notes）

- IPA（情報処理推進機構）とJPCERT/CCが共同管理する脆弱性情報ポータルサイト
- 日本製のソフトウェアに関する情報が充実



iDefenseセキュリティインテリジェンスサービス

- Verisign社が有料で提供するポータルサイト
- 脆弱性情報のほか、アナリストの分析レポート、PoC、ハクティビストの活動レポート等、動向調査に有用な情報が揃っている

iDefenseセキュリティインテリジェンスサービス

- ハクティビストの活動レポートの例

1月28日

種別: Defacement
情報元: Twitter
首謀者: @AnonManifest, Anonymous Brazil
詳細: アノニマスブラジルのTwitterユーザ@AnonManifestが、サンパウロ州政府のポータルサイト (http://www.sp.gov.br) を改ざんしたと伝えました。攻撃理由は、2014年にブラジルで開催されるFIFAワールドカップへの反対です。iDefenseのアナリストは、対象ドメインが改ざんされているのを確認しました。

脆弱性対策の実施手順

① 脆弱性の洗い出し
- 脆弱性診断による確認
- ソフトウェアのバージョンから、影響のある脆弱性を確認

② 脆弱性の調査
- 対策手段の確認（セキュリティ修正パッチの公開状況）
- 深刻度の確認（CVSSの値、エクスプロイトコードの公開状況）

③ 対策の実施
- セキュリティ修正パッチの適用
- セキュリティ製品、ネットワーク機器による対策の実施

④ 対策が有効であることの確認
- PoCを使用して脆弱性が排除されたことを確認
- 脆弱性診断による確認

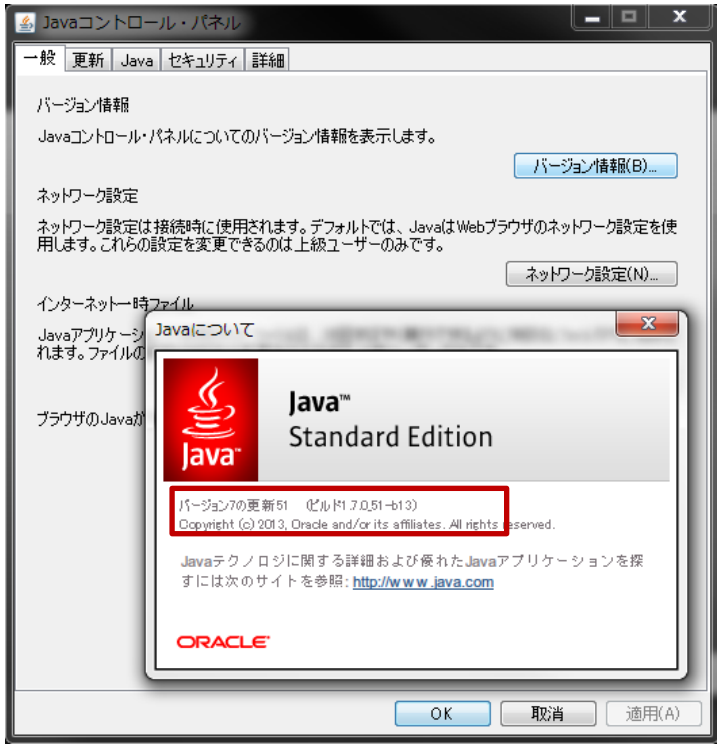
ソフトウェアのバージョン確認方法（Windows）

- ソフトウェアによって確認方法が異なる
- 多くの場合は、ソフトウェアを起動し、ツールバーの「ヘルプ」「設定」などに「バージョン確認」が用意されている

InternetExplorer10の場合
設定 -> バージョン情報

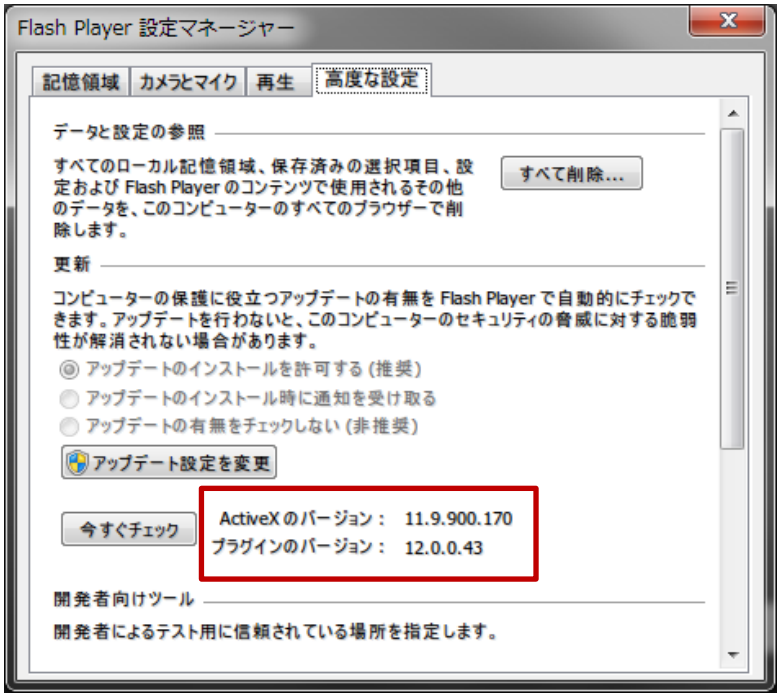
ソフトウェアのバージョン確認方法（Windows）

- Javaの場合
  - コントロールパネル -> Java -> バージョン情報



ソフトウェアのバージョン確認方法（Windows）

- Adobe Flash Playerの場合
  - コントロールパネル -> Flash Player -> 高度な設定



【注意】FlashPlayerは2種類存在する
Activex： Internet Explorer、sleipnirなど
プラグイン: Firefox、Operaなど

ActiveXのバージョン
プラグインのバージョン
それぞれが表示されている

ソフトウェアのバージョン確認方法（Linux）

- カーネルのバージョン確認

  # uname –r

```
# uname –r
2.6.32-358.6.2.el6.i686    OSのリリース番号を表示
```

- パッケージ管理ソフトウェアで確認

  RPM（RedHat Package Manager）の場合
  # rpm –qi [ソフトウェア名]

```
# rpm -qi httpd
Name        : httpd                        Relocations: (not relocatable)
Version     : 2.2.15                            Vendor: CentOS
Release     : 29.el6.centos                  Build Date: 2013年08月14日 02時28
分20秒
--- snip ---
```

ソフトウェアのバージョンから脆弱性を確認

- NVDを利用
  - CPE（Common Platform Enumerations）で検索
    - CPE：ハードウェア、ソフトウェアなどを識別するための共通の名称基準
    - 例）cpe:/a:adobe:acrobat_reader:10.0.1
      （Adobe Reader 10.0.1 の場合）

- JVN iPediaを利用（日本製品に多く対応）
  - ベンダ名と製品名から検索
    ※ 一部カタカナ表記のため、注意が必要
    「マイクロソフト」、「アドビシステムズ」など

脆弱性の調査
（CVE-2013-3906の調査例）

- CVE-2013-3906の概要
  - （MS13-096）Microsoft Graphics コンポーネントの脆弱性により、リモートでコードが実行される
    <https://technet.microsoft.com/ja-jp/security/bulletin/ms13-096>
- アドバイザリ公開日
  - ２０１３年１２月１１日

脆弱性の調査
（CVE-2013-3906の調査例）

- 深刻度の確認
  - CVSSの基本値
    <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-3906>

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)

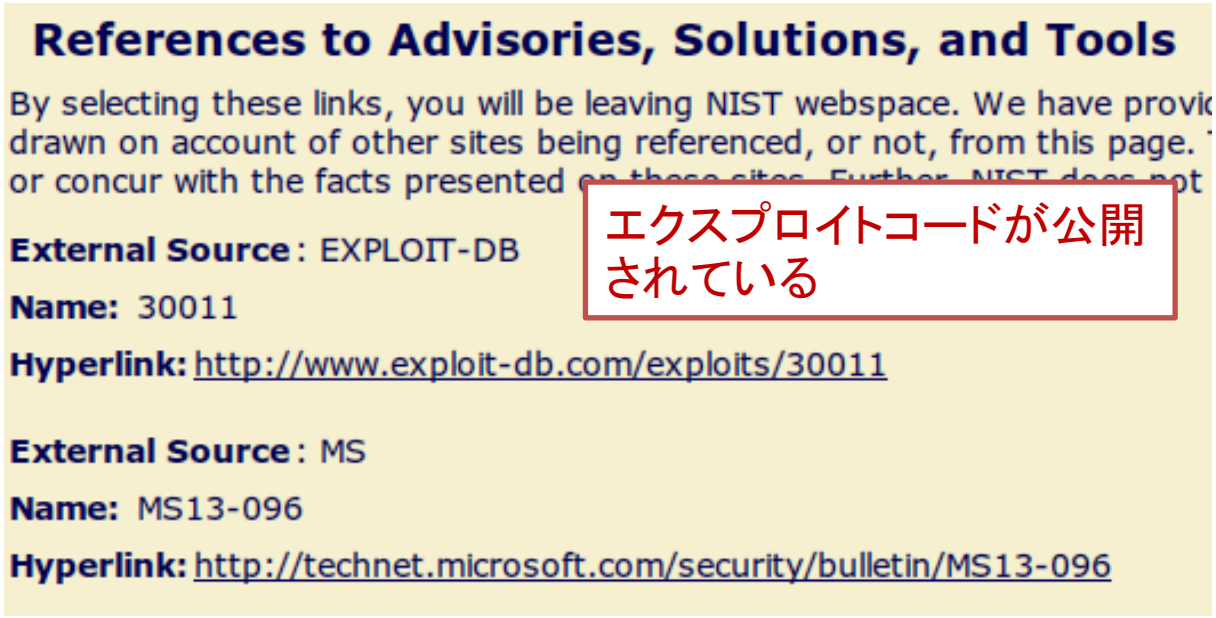
Impact Subscore: 10.0

Exploitability Subscore: 8.6

HIGHであり、深刻な脆弱性であることが分かる

脆弱性の調査
（CVE-2013-3906の調査例）

- 深刻度の確認
  - エクスプロイトコードの公開状況
    <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-3906>



脆弱性の調査
（CVE-2013-3906の調査例）

- CVE-2013-3906の対策手段の確認
  - ベンダ情報を確認

    < https://technet.microsoft.com/ja-jp/security/bulletin/ms13-096 >

更新プログラムに関する情報

⊞ 検出および展開ツールとガイダンス

⊟ セキュリティ更新プログラムの展開

影響を受けるソフトウェア

影響を受けるソフトウェア用の特定のセキュリティ更新プログラムについては、該当リンクの情報を参照してください。

⊟ Windows Vista (すべてのエディション)

参照表

次の表では、このソフトウェア用のセキュリティ更新プログラムの情報を記載しています。

セキュリティ更新プログラムのファイル名	すべてのサポートされている 32 ビット版の Windows Vista: Windows6.0-KB2901674-x86.msu
	すべてのサポートされている x64-based エディションの Windows Vista: Windows6.0-KB2901674-x64.msu

更新プログラムが公開されている

脆弱性の調査
（CVE-2013-3906の調査例）

- iDefenseセキュリティインテリジェンスサービスを利用した調査
  - アナリストによる分析レポート
  - 世界規模の攻撃確認情報
  - エクスプロイトコードの可用性
  - 対策情報

脆弱性の調査
（CVE-2013-3906の調査例）

- iDefenseセキュリティインテリジェンスサービスを利用した調査
  - 脅威レポート:
    「CVE-2013-3906とインド人ハッカーによるOpHangover の関係」