

【不具合報告】 Nablarch 汎用データフォーマット XXE脆弱性について

この度、Nablarch 汎用データフォーマット機能について、後述する脆弱性が発見されました。本報告書にて、脆弱性の内容、システム影響、および対応方法についてご報告致します。

1. 汎用データフォーマット機能の概要

システムで扱う多様なデータ形式に対応した汎用の入出力ライブラリ機能を提供します。

- ・ 固定長
- ・ 可変長(csvやtsvなど)
- ・ JSON
- ・ XML

Nablarch公開ドキュメント「汎用データフォーマット」

https://nablarch.github.io/docs/LATEST/doc/application_framework/application_framework/libraries/data_io/data_format.html

2. 本脆弱性について

2.1. 脆弱性の概要

汎用データフォーマット機能にて、XML文書を読み込むときにXXE(XML External Entity)攻撃を受ける可能性があります。

XXE攻撃はNablarch特有のものではなく一般的な攻撃方法となります。

XML文書の構造を定義するためのDTD(Document Type Definition)の機能を利用して攻撃を行います。

詳細は以下のサイト等を参照ください。

[https://www.owasp.org/index.php/XML_External_Entity_\(XXE\)_Processing](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing)

2.2. 本脆弱性が発生するNablarchのバージョン

Nablarch 5, 5u1～5u13で発生します。

2.3. 本脆弱性の対象となるシステム

汎用データフォーマット機能を利用してXML文書を入力しているシステム

典型的な使用ケースとして以下が挙げられます。

- ・ XML電文を受け取るHTTPメッセージングシステム
- ・ XMLファイルを入力する処理(バッチ,画面等の処理形態に依存しない)

2.4. 本脆弱性によるシステム影響

XML文書を入力する時にXXE攻撃を受ける可能性があります。

攻撃パターンは多岐に渡りますが、情報漏えいやシステム停止が発生する恐れがあります。

2.5. 攻撃方法

典型的には以下のような攻撃が挙げられます。

- ・ 本来外部から読み取れないはずのファイルをシステム経由で読み取る
- ・ システムのスローダウンないしシステム停止を発生させる

※上記は一例です。詳細はOWASP等のサイトを参照ください。

[https://www.owasp.org/index.php/XML_External_Entity_\(XXE\)_Processing](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing)

【ファイル読み取りの例】

以下の例では、<root>要素にsecret.txtの内容が展開されます。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE name [
  <!ENTITY sc SYSTEM "file:///path/to/secret.txt">
]>
<root>&sc;</root>
```

【DoS攻撃の例】

以下の例では、処理が戻らないリソースに意図的にアクセスすることで、システムの処理を停止させます。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///dev/random" >]><foo>&xxe;</foo>
```

3. 不具合原因と対応方法 (Nablarch)

NablarchはXML文書を扱うためにXMLライブラリ(JAXP)を使用しています。

デフォルトではDTDが使用可能になっており、これを明示的に使用不可に設定していないことが不具合原因となります。

よって、対処としては、XMLライブラリを使用する際にDTDを使用できない設定を行います。

※この対処方法はOWASPが提示した対応方法のうち第一に推奨されるものです。

[https://www.owasp.org/index.php/XML_External_Entity_\(XXE\)_Prevention_Cheat_Sheet#JAXP_DocumentBuilderFactory_2C_SAXParserFactory_and_DOM4J](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet#JAXP_DocumentBuilderFactory_2C_SAXParserFactory_and_DOM4J)

バージョンアップ後は、DTDを使用したXML文書が入力された場合は読み込み処理が停止し、例外が発生するようになります。

これによりXXE攻撃が無効になります。

DTDを使用したXML文書が入力された場合、入出力データ不正により処理が継続できないことを示す例外クラス

nablarch.core.dataformat.InvalidDataFormatException がスローされます。

これは、不正なフォーマットのXML文書を入力した場合と同じ動作です。

4. 対応方法（Nablarch利用プロジェクト）

4.1. 基本的な対応方法

本脆弱性の対象となるシステムは、最新版へのバージョンアップを行ってください。
バージョンアップにより、DTDが使用できなくなりXXE攻撃が無効になります。

もし意図的にDTDを使用しているシステムがあれば、XML Schema等の代替技術に置き換える等の対処を行い、DTDの使用を止めるようにしてください。

4.2. バージョンアップが困難な場合の回避方法

推奨はしませんが、「XXE攻撃を受ける可能性が全くない」と判断できる場合に限り、リスクを許容した上でバージョンアップを行わないという選択肢もあり得ます。

【XXE攻撃を受けないと判断する例】

- ・ システム内部で作成したXML文書しか扱わない
- ・ システム間で事前に取り決めを行ったフォーマットだけしか扱わない

このように、XXE攻撃に繋がるようなDTDが一切使われない場合は、脆弱性を攻撃される可能性がないと考えてリスクを許容するという判断もあり得えます。

※ただし、今後のシステム改修で扱うXML文書の種類が増える可能性があったり、内部の関係者による攻撃の可能性には対応できません。

DTDが使用されないことが保証できない場合、回避方法はありません。

4.3. 本件に関わるJDKのバグについて

以下のバージョンのJDKにはAPIに不具合があり、DTDの無効化を行った場合にNullPointerExceptionが発生します。

- ・ JDK6 6u65 未満
- ・ JDK7 7u6 b15 未満

本バグを回避するには、JDKのバージョンをアップする必要があります。
不具合詳細は 以下を参照ください。

JDK-7157610 : NullPointerException occurs when parsing XML doc

https://bugs.java.com/bugdatabase/view_bug.do?bug_id=7157610