令和５年(2023年)12月14日

各　　位

滋賀県警察サイバー攻撃対策プロジェクト
(警備第一課　担当　川瀬、西山)

Apache Strusts 2における外部からアクセス可能なファイルの脆弱性について

平素は警察行政に格段の御協力を賜り、誠にありがとうございます。

今回は、

・Apache Strusts 2における外部からアクセス可能なファイルの脆弱性
(CVE-2023-50164)

について、注意喚起及び

・令和５年11月期レポート_最近の情勢について

・令和５年11月期観測資料

について、別添資料を送らせていただきますので対策の参考としてください。

本件にかかる被害を認知した場合には、下記連絡先へ御相談いただきますようお願い申し上げます。

〈問合せ先〉
滋賀県警察本部警備部警備第一課内
滋賀県警察サイバー攻撃対策プロジェクト
電話　077-522-1231　(内線 5793)
Email pph-shiga@post.cyberpolice.go.jp

機密性1（低）情報
（重要インフラ事業者等への配布可）

令和5年12月11日

Apache Struts 2における外部から アクセス可能なファイルの 脆弱性(CVE-2023-50164)について

警察庁サイバー警察局
情報技術解析課
サイバーテロ対策技術室

1. 概要

Apache Software Foundationは12月7日(現地時間)に同団体のWebアプリケーションであるApache Struts 2における外部からアクセス可能なファイルの脆弱性(CVE-2023-50164)についてのアドバイザリを公開した。[5.参考(1)]

- 本脆弱性を悪用することで、攻撃者がファイルアップロードパラメータを操作することによりパストラバーサルの問題が発生し、状況によってはリモートコード実行を引き起こすような悪意の有るファイルをアップロードすることが可能となる。
- 同団体は本脆弱性を悪用した攻撃の発生を確認していない。

2. 脆弱性の深刻度

Apache Software Foundationによると本脆弱性の深刻度は**critical（緊急）**レベルであるとしている。
[5.参考(1)]

3. 影響範囲

- Apache Software Foundationが公開している情報によると、本脆弱性の影響を受ける製品・バージョン及び脆弱性が修正されたバージョンは以下のとおり。

影響を受けるバージョン	脆弱性に対応したバージョン
2.0.0から2.3.37	なし（EOL）
2.5.0から2.5.32	2.5.33
6.0.0から6.3.0	6.3.0.2

※すでにサポートが終了(EOL)を迎えているバージョン2.0.0から2.3.37についても本脆弱性の影響を受けることから、同団体は最新のサポート対象バージョンへアップデートを推奨している。最新の情報及び詳細については、Apache Software Foundation等のウェブサイト[5.参考(2)~(4)]を参照

4. 対策

- 脆弱性が修正された最新バージョンへ速やかに更新する。
  [5.参考(3)]

5. 参考

(1) S2-066 - Apache Struts 2 Wiki
https://cwiki.apache.org/confluence/display/WW/S2-066

(2) [ANN]Apache Struts 6.3.0.2&2.5.33
https://lists.apache.org/thread/yh09b3fkf6vz5d6jdgrlvmg60lfwtqhj

(3) Download a Release of the Apache Struts
https://struts.apache.org/download.cgi#struts-ga

(4) JVNVU#96961218_ Apache Struts 2における外部からアクセス可能なファイルの脆弱性（S2-066）
https://jvn.jp/vu/JVNVU96961218/index.html

6. 変更履歴

- 12月11日　初版