

FutureVulsのSSVC機能を用いたDev/Ops目線の運用

vuls.biz



運用者は **immediate** 検知の通知を受けてログイン。決定木、プロセスやPort開放状態、IPSルール有無、脆弱性情報、CERT注意喚起、Exploit情報等を画面から確認して対応する。



Future Vuls Immediate

Immediateタスク新規検知
該当する脆弱性への早急な対応を推奨

CVE-2020-25213

File Manager 6.0-6.9 - Unauthenticated Arbitrary File Upload leading to RCE

タスクを確認する

対応期限

2023-09-30T01:32:01Z

検知したサーバ名

cy-test-10.31.43 (グループ名: e2e-test / デフォルト担当者: cy-biro_2023/9/25 16:08:13)

関連するパッケージ

ソフトウェア名	バージョン
cpes/ia:webdesig:file_manager	wordpress

下のSSVC Decision PointによってImmediateと分類されました

Exploitation	Exposure	Utility	Density	Automatable	Human Impact
active	open	concentrated	no	no	very_high

◇決定木の判断理由

- ・攻撃がアクティブ
 - ・インターネット公開システム
 - ・リモートコード実行
 - ・重要システム
- であるため

immediateと判断された



task #2404779

タスク詳細

初回検知日時: 2023-08-01T01:18:00Z
検出方法: UbuntuAPIMatch (信頼度: 100%)

CVE ID: CVE-2023-38408
サーバ名: c4c56a44e278

ステータス: NEW
優先度: MEDIUM

対応予定日: 2023/10/10
対応期限: 2023/10/10

関連するソフトウェア

ソフトウェア名	バージョン	アップデート	リポート	location	バッチ	初回検知日時	影響を受けるプロセス
openssl_client	1.8.9p1-3ubuntu0.1	(最新)	-	-	fixed (修正: 1.8.9p1-3ubuntu0.3)	2023/02/06 11:41	sshd (PID: 7)
openssl_server	1.8.9p1-3ubuntu0.1	(最新)	-	-	fixed (修正: 1.8.9p1-3ubuntu0.3)	2023/02/06 11:41	sshd (PID: 1 PORT: *22)
openssl_sftp_server	1.8.9p1-3ubuntu0.1	(最新)	-	-	fixed (修正: 1.8.9p1-3ubuntu0.3)	2023/02/06 11:41	

アップデートコマンド: ANSIBLE PLAYBOOK

サードパーティのリポジトリからインストールされたソフトウェアの場合は、誤検知の可能性がります

SSVC

Priority	全てのリソースを集中し必要に応じて組織の通常業務を停止して可能な限り迅速に対応する	immediate
Exploitation	実行の意図を確認した状態でできる情報がある	active
Exposure	インターネットから制限なしにアクセス可能なシステム	open
Utility	攻撃が効果的	efficient
Utility Density	重要情報が集中している (例: サーバ、データベース)	concentrated
Utility Automatable	攻撃を自動化できない (例: サーバ、システム)	no
Human Impact	最悪業務に長期影響が出る (例: 最悪システム)	high

対象機器や対応期限等

「ソフトウェア名」
「プロセス有無」
「Port開放状況」

CVE-2018-11776

CISA KEY: 米政府のサイバーセキュリティ・インフラセキュリティの脆弱性です。この脆弱性は攻撃に悪用されればリスクのある脆弱性です。早急な対応が必要です

サマリ

Red Hat	JVN	NVD	Ubuntu
9.8	-	8.1	M

Apache Struts2 における任意のコードが実行可能な脆弱性

Apache Struts2 には、ユーザ入力の不十分な検証に起因する、任意のコードが実行可能な脆弱性が存在します。詳細は<https://www.apache.org/confluence/display/WW2-05?target=black+ペンダ>を参照してください。なお、本脆弱性の攻撃コードが公開されています。

CVSS

RED HAT V3	NVD V3	NVD V2
9.8	8.1	8.1

評価尺度	攻撃成立条件	評価値	レベル
攻撃区分(Av)	ネットワーク経由でリモートから攻撃可能	ネットワーク	高
攻撃条件の複雑さ(AC)	特別な攻撃条件を必要とせず、対象コンポーネントに常に攻撃可能	低	高
必要な特権レベル(PR)	特別な特権なしで攻撃可能	不要	高
ユーザー間レベル(U)	ユーザーが何もしなくても脆弱性が攻撃される可能性がある	不要なし	高
スコープ(S)	影響範囲が同じ管理権限の範囲に留まる	高	高
機密性への影響(C)	機密情報や重要なシステムファイルが参照可能であり、その問題による影響が全体に及ぶ	高	高
完全性への影響(I)	機密情報や重要なシステムファイルの改ざんが可能で、その問題による影響が全体に及ぶ	高	高
可用性への影響(A)	リソースを完全に枯渇させたり、完全に停止させることが可能	高	高

↓ CVSSスコアの再計算

攻撃コード (信頼度: high)

https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/http/struts2_namespace_ognl.rb

This module exploits a remote code execution vulnerability in Apache Struts version 2.3 - 2.3.4, and 2.5 - 2.5.16. Remote Code Execution can be performed via an endpoint that makes use of a redirect action. Note that this exploit is dependent on the version of Tomcat running on the target. Versions of Tomcat starting with 7.0.88 currently don't support payloads larger than ~7.5kb. Windows Meterpreter (信頼度: HIGH)

「脆弱性情報」
「CERT注意喚起」
「Exploit情報」

FutureVulsのSSVC機能を用いたCSIRT目線の管理

vuls.biz



CSIRTは全社横断で **immediate** と **out-of-cycle** の対応状況を確認し、対応期限が超過したタスクには一括で対応を催促する。脆弱性管理の工数を削減可能。

all	▼	ダッシュボード(beta)	脆弱性	タスク	ソフトウェア
すべて					
タスクを非表示 非表示の解除 タスクを編集 データ更新 列一覧 フィルター 行間隔 エクスポート					
<input type="checkbox"/>	SSVC PRIORITY	対応期限(タスク) ↑	対応予定日	ステータス	CVE ID
<input type="checkbox"/>	immediate	2023/02/03	2023/02/02	new	CVE-2021-35587
<input type="checkbox"/>	immediate	2023/02/08	-	new	CVE-2018-0180
<input type="checkbox"/>	immediate	2023/02/08	-	new	CVE-2018-0172
<input type="checkbox"/>	immediate	2023/02/08	-	new	CVE-2018-0179

immediate に分類されたタスクのうち「未対応」かつ「対応期限が超過している」などでフィルタ

タスクの担当者に対応を催促する。
一つの操作で全社の担当者に指示が可能。



脆弱性 タスク ソフトウェア

データ更新 列一覧 フィルター 行間隔 エクスポート

タスクを編集

優先度

対応予定日
年/月/日 ☐ 対応日時をクリア

対応期限
年/月/日 ☐ 対応期限をクリア

警戒タグが設定されている場合は更新をスキップします

コメント投稿

Immediateのタスクが放置されています。対応してください。既に対応済みの場合はタスクのステータスを変更して、タスクコメントに詳細を記載ください。

グループ全員にコメント追加をメール通知

キャンセル タスクを更新