ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

● Apache Tomcatに任意コード実行の脆弱性、既に悪用も

https://jvn.jp/vu/JVNVU93567491/
https://codebook.machinarecord.com/threatreport/37760/
https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.3
https://lab.wallarm.com/one-put-request-to-own-tomcat-cve-2025-24813-rce-is-in-the-wild/

このニュースをザックリ言うと･･･

- 3月11日(日本時間)、JVNよりApache Tomcatに脆弱性(CVE-2025-24813)が存在するとして注意喚起が出されています。

- 悪用により、「リモートコード実行、セキュリティ上重要なファイルの表示やコンテンツ挿入の可能性」があるとしており、また同17日(現地時間)、セキュリティベンダーのWallam社によれば、脆弱性を悪用する攻撃や、攻撃コードの公開が既に確認されているとのことです。

- 2月にTomcatの開発元より修正バージョン(11.0.3/10.1.35/9.0.99)がリリースされていますが、3月上旬リリースの最新バージョンである11.0.5/10.1.39/9.0.102へのアップデートが強く推奨されます。

AUS便りからの所感等

- Tomcatは、サーバーサイドでJavaによるWebアプリケーション(Servlet・JSP)を実行するために現在も良く用いられるソフトウェアであり、StrutsやSpring Frameworkといったフレームワーク等がTomcat上で稼働します。

- Tomcatにおいては2024年12月にもリモートコード実行につながる等複数の脆弱性(CVE-2024-50379, CVE-2024-54677, CVE-2024-56337)が報告され、11.0.2/10.1.34/9.0.98がリリースされる等、不定期にセキュリティアップデートが行われています。

- ともあれ、脆弱性の根本的な対策として、Tomcatはもちろん各種フレームワークやWebサーバーソフトウェア、OS自体に至るまで各種ソフトウェアを常時最新のバージョンに保つことと、サーバー自体やUTMによるパケットフィルタリングあるいはWebアプリケーションファイアウォール(WAF)の設定とをそれぞれ確実に行うことが重要です。

JVNVU#93567491
Apache Tomcat partial PUTにおけるリモートコード実行、情報漏えいや改ざんの脆弱性(CVE-2025-24813)

概要
Apache Tomcatのpartial PUTの元の実装には、リモートコード実行、情報漏えいや改ざんとなり得る脆弱性が存在します。

影響を受けるシステム
- Apache Tomcat 11.0.0-M1から11.0.2まで
- Apache Tomcat 10.1.0-M1から10.1.34まで
- Apache Tomcat 9.0.0.M1から9.0.98まで

詳細情報
Apache Tomcatのpartial PUTの元の実装では、ユーザーが指定したファイル名とパスを基にパス区切り文字を「」に置き換えた一時ファイルが使用されています。このため、特定の条件下で、リモートコード実行、セキュリティ上重要なファイルの表示やコンテンツ挿入の可能性があります。(CVE-2025-24813、CWE-44、CWE-502)

想定される影響
以下のすべての条件が成立する場合、セキュリティ上重要なファイルの表示やコンテンツ挿入の可能性があります。
- デフォルトサーブレットの書き込みが有効(デフォルトで無効)
- partial PUTをサポート(デフォルトで有効)
- セキュリティ上重要なアップロード対象のURLが、パブリックアップロード対象URLのサブディレクトリである
- 攻撃者がアップロードされるセキュリティ上重要なファイルの名前を知っている
- セキュリティ上重要なファイルがpartial PUTでアップロードされる

codebook

Threat Report #Silobreaker-CyberAlert #脆弱性

Apache TomcatのRCE脆弱性、攻撃で悪用される：CVE-2025-24813

佐々山 Tacos 2025.03.18

Apache TomcatのRCE脆弱性、攻撃で悪用される：CVE-2025-24813

Wallarm – March 14, 2025

Apache TomcatにおけるRCEの脆弱性CVE-2025-24813の悪用が開始され、公開エクスプロイトも登場していることをWallarmが報告。当初中国語フォーラムのユーザー「iSee857」によってリリースされたPoCエクスプロイトは、既にGitHubでも利用可能になっているという。

このエクスプロイトは、①PUT APIリクエストを通じたシリアライズされたJavaセッションのアップロードと、②GETリクエスト内で有害なセッションIDを参照することによるデシリアライゼーションのトリガー、という2つのステップで構成されている。攻撃には、Tomcatのデフォルトのセッション永続化メカニズムと、部分的なPUTリクエストの処理が有効である状態を悪用して行われるという。

●auひかりホームゲートウェイ「HGW-BL1500HM」に脆弱性…ファームウェアアップデートを

https://internet.watch.impress.co.jp/docs/news/2000036.html
https://jvn.jp/jp/JVN04278547/index.html
https://kddi-tech.com/contents/appendix_L2_06.html

このニュースをザックリ言うと･･･

- 3月19日(日本時間)、JVNより、KDDI「auひかり」で提供されるホームゲートウェイ「HGW-BL1500HM」に複数の脆弱性が存在するとして注意喚起が出されています。
- 脆弱性はUSBストレージファイル共有機能等に存在し、任意のスクリプトやコードの実行、製品上のファイルの窃取・改ざん・削除の可能性があるとされています。
- 同18日にKDDIよりファームウェアの修正バージョン(002.004.010)がリリースされており、アップデートが強く推奨されます。

AUS便りからの所感

- 脆弱性はクロスサイトスクリプティング(XSS)(CVE-2025-27567, CVE-2025-27574)およびパストラバーサル(CVE-2025-27718, CVE-2025-27726, CVE-2025-27932)の可能性があるとのことですが、XSSの脆弱性に対してはその悪用に誘導されることのないよう、管理画面等へのログイン専用にプライベートモード(シークレットウィンドウ)を使う等を心掛けましょう。
- ブロードバンドルーター等のネットワーク機器によってはサポート終了後に脆弱性が発表され、ファームウェア更新が提供されないケースも起こり得ますので、組織内で使用している全ての機器について随時サポート情報のチェックを行うとともに、サポート終了した機器を確実にリプレースする管理体制も整えることが肝要です。

Impress Watch

> **auひかりのホームゲートウェイ「HGW-BL1500HM」に複数の脆弱性、最新版ファームウェアへの更新を**
>
> 山田 貞幸　2025年3月19日 16:10
>
> KDDIが「auひかり」のホームゲートウェイとして提供する「HGW-BL1500HM」に複数の脆弱性があるとして、同社および脆弱性対策情報ポータルサイト「JVN（Japan Vulnerability Notes）」が情報を公開した。最新版のファームウェアに更新することで対策できる。
>
> 対象となるのは、HGW-BL1500HMのファームウェアバージョン「002.002.003」以前。なお、同製品はファームウェア自動更新機能を備えており、特に操作をしなくても3月18日に配信された最新バージョンのファームウェア「002.004.010」に更新されるとしている。念のため、自宅で使用中の製品バージョンを確認しておくことが望ましい。

● 2月フィッシング報告件数は141,223件、再度増加の可能性に警戒

https://www.antiphishing.jp/report/monthly/202502.html

このニュースをザックリ言うと･･･

- 3月17日(日本時間)、フィッシング対策協議会より、2月に寄せられたフィッシング報告状況が発表されました。
- 2月度の報告件数は141,223件で、1月度(https://www.antiphishing.jp/report/monthly/202501.html)の136,169件から5,054件増加しています。
- フィッシングサイトのURL件数は22,518件で1月度(43,534件)から21,016件減少、使用されるTLD(トップレベルドメイン名)の割合は .com(約45.0%)、.cn(約33.7%)で合わせて約78.7%、これに続く .goog(約9.0%)を含めると約87.8%となっています。
- 悪用されたブランド件数は99件で1月度(89件)から10件増加、最も割合が多かったブランドとしてはAmazonとPayPayがそれぞれ全体の約28.3%と13.8%、次いでApple、オリコ、NHKと合わせて約55.5%、さらに1,000件以上報告された22ブランドまで含めると約91.0%を占めたとのことです。

AUS便りからの所感

- 中国の旧正月が関係してか、月間の件数では大きな落ち込みをみせた1月から微増した程度でしたが、2月中旬以降報告数が急増しているとのことで、3月以降には再び20万件を超える可能性が高く、警戒が必要でしょう。
- 同協議会から2022年8月に注意喚起が出されたことがある(https://www.antiphishing.jp/news/alert/googletranslate_20220809.html)「Google翻訳の正規URL(https://translate.google.com/translate?●●●●)からフィッシングサイトに誘導する」ケースも増加している模様で、2月度についてはフィッシングサイトURLの約29.4%で悪用されたとのことです。
- また日本データ通信協会の迷惑メール相談センターには日々20件以上のフィッシングメールが掲載されており(https://www.dekyo.or.jp/soudan/contents/news/alert.html)、利用しているサービスについて不審なメールを受信した際はこういった情報等と文言が一致するか確認するとともに、本物のサービスのサイトへは事前に登録したブラウザーのブックマークやスマホアプリからアクセスする等、慎重に行動することを日々心掛けましょう。

フィッシング対策協議会
Council of Anti-Phishing Japan