プレスリリース
報道関係社各位

2022年1月12日
株式会社ビットフォレスト

脆弱性診断ツール「VAddy」、Apache Log4jの脆弱性（CVE-2021-44228）検査を全ユーザーに提供を拡大

株式会社ビットフォレスト（東京都千代田区　代表取締役 高尾都季一　以下、ビットフォレスト）は、クラウド型Web脆弱性診断ツール「VAddy」の無料トライアルを含む全てのプランにおいて、Apache Log4jの脆弱性（CVE-2021-44228）検査機能の提供を開始しました。

VAddyではApache Log4jの脆弱性（CVE-2021-44228）の公表の翌営業日である2021年12月13日からVAddy Enterpriseプラン／Enterprise+プランをご利用のお客様向けに先行してApache Log4jの脆弱性（CVE-2021-44228）に対する検査機能を提供してきました。Apache Log4jは多くのJavaプログラムで利用されており、本脆弱性の公表から約一ヶ月経過した今日でも自社のWebサービスにてApach Log4jの利用状況を把握しきれないお客様も多い状況です。本脆弱性は外部から簡単にスキャンや実行ができ、かつ重大な影響を与える脆弱性であることから、VAddyでも全ユーザーが検査できるように対象ユーザーを拡大しました。

なお、本機能は2022年1月31日までの期間限定提供を予定していますのでまだVAddyアカウントをお持ちでないお客様はお早めに無料トライアルをお申込みください。すでにVAddy有料プランをご利用中のお客様は、特別な設定無しでApache Log4j検査をご利用いただけます。

・VAddy 無料トライアル
https://console.vaddy.net/ja/signup

■VAddyにおけるApache Log4j検査

これまでのVAddyでは特定のフレームワークやライブラリを想定した検査には対応していませんでした。しかしながら、Apache Log4jは多くのJavaプログラムで利用されいているため影響が広範囲に及びうること、また本脆弱性を狙った攻撃には高度なスキルを要しないことなどから、例外的な対応として本脆弱性への検査機能を緊急リリースしました。

全ユーザーが対象になったことで、VAddy Enterpriseプラン／Enterprise+プランをご利用のお客様だけではなく、Professionalプラン、Starterプラン、VAddyをご検討中のトライアルの方も追加料金なしでApache Log4jの検査が実行できます。
VAddyにおけるApache Log4j脆弱性の検査機能の詳細は下記のブログを参照ください。
https://blog-ja.vaddy.net/post/vaddy-log4j-scan

なお、この問題はApache Log4jの最新バージョンへのアップデートやセキュリティパッチの適用によって回避できるため、本機能は2022年1月31日までの期間限定提供となります。

■クラウド型Web脆弱性診断ツール「VAddy」について

「VAddy」は クラウド型 WAF（Web Application Firewall）国内市場売上シェアNo.1を誇る「Scutum（スキュータム）」の開発チームが開発した、今もっとも手軽で高速な純国産のクラウド型 Web アプリケーション脆弱性診断ツールです。

従来の脆弱性診断ツールのように導入前トレーニングや複雑な設定作業を必要とせず、簡単なブラウザ操作だけで未経験者でも最短10分で初回の検査を開始できる手軽さが支持され、数人規模のスタートアップ企業から数万人規模の大企業まで幅広く利用されています。

■Apache Log4jの脆弱性（CVE-2021-44228）とは

オープンソースのロギングライブラリ「Apache Log4j」に、任意のコード実行の脆弱性（CVE-2021-44228）があることが発表されました。

※JPCERT/CC Apache Log4jの任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210050.html

この脆弱性は文字通り、第三者がリモートからApach Log4jを利用しているサーバー上で任意のコードを実行できるというものです。

任意のコード実行の危険性は言うに及ばず、今回の脆弱性によって外部から入力されたアドレスに対してDNSの名前解決やLDAPサーバーへのアクセスも行われることから、DNSの名前解決時にサーバ側の環境情報（データベースパスワードやAPIキーなど）を名前解決のFQDNに含めることで環境情報の漏洩につながります。

クラウド型WAF「Scutum」のプレスリリースでもご案内している通り、2021年12月12日までにScutumにおいて483サイト2553件以上の攻撃を検知・防御しており、VAddyでも本脆弱性は緊急対策を必要とするものと認識しております。

※クラウド型WAF「Scutum」プレスリリース
https://www.scutum.jp/topics/images/pressrelease20211213.pdf

●本文内でご紹介した製品等について

VAddy 公式Webサイト：https://vaddy.net/ja/
Scutum公式Webサイト：https://www.scutum.jp/

●お問い合わせ
株式会社ビットフォレスト
VAddy事業部
担当 西野
info@vaddy.net
03-5577-2032

企業情報

【ビットフォレストについて】

https://www.bitforest.jp/

社名：株式会社ビットフォレスト

代表者：代表取締役　高尾 都季一

事業内容：Webアプリケーションセキュリティ製品の開発、販売

リリースに関する報道機関からの問い合わせ先

■株式会社ビットフォレスト VAddy事業部　広報担当：西野

電話：03-5577-2032

メールアドレス：info@vaddy.net

Twitter VAddyアカウント：@vaddynet

Facebook VAddyページ：https://www.facebook.com/vaddynet/