



2026 年 10 月 27 日
株式会社ユビキタス AI
We-Fuzz Inc.

PRESS RELEASE

ユビキタス AI が販売するセキュリティ脆弱性検証ツール「Penzzzer」が、未知の情報漏えい脆弱性を発見し、IoT・産業機器の監視基盤に警鐘

—SNMP エージェント「mini-snmpd」に潜む「MIBleed」は、認証不要で Community String が漏えいする恐れ—

ファuzzング・ペネトレーションテストツール「Penzzzer」の開発元である米国 We-Fuzz Inc.（以下「We-Fuzz 社」）と、日本国内における同製品の提供および IoT デバイスセキュリティ検証サービスを手掛ける株式会社ユビキタス AI（本社：東京都新宿区、代表取締役社長 CEO：大吉裕太、以下「ユビキタス AI」）は、We-Fuzz 社が自社製品「Penzzzer」を用いて実施した脆弱性検証の結果、軽量 SNMP エージェントソフトウェア「mini-snmpd」（バージョン 2.0 以下）に、未初期化メモリ情報漏えいの脆弱性を新たに発見したことを共同で発表します。

We-Fuzz 社はこの脆弱性を「MIBleed」と命名し、責任ある開示の方針（Responsible Disclosure）に基づき mini-snmpd の開発元へ報告しました。この報告を受けて、修正版となる mini-snmpd 2.1 がリリースされています。

工場やオフィスのネットワーク機器を遠隔から見守るために世界中で広く使われているソフトウェアに、長年見過ごされてきた不具合が見つかりました。例えるなら、窓口に問い合わせたときに、自分宛での回答と一緒に、別の人が直前に受け取ったはずの回答の切れ端まで、紛れて渡されてしまうようなものです。その「切れ端」の中には、機器を管理するための合言葉（パスワードに相当する情報）が含まれている可能性があり、特別な攻撃ツールを使わなくても、ネットワーク越しに特定の問い合わせを送るだけで再現しうるため、幅広い利用者に注意が必要です。

mini-snmpd はネットワーク機器や IoT デバイスの死活監視・状態把握に広く用いられている SNMP エージェントです。今回発見された脆弱性は、世界中の監視環境に潜在的な影響を及ぼす可能性があります。なお、本脆弱性の技術的な詳細は、2026 年 11 月 18 日（水）に国際情報セキュリティカンファレンス「CODE BLUE 2026」において、We-Fuzz 社より発表される予定です。

■MIBleed とは

MIBleed は、攻撃者が細工した SNMP リクエストを送信するだけで、本来返されるべき応答データに加えて、サーバーが過去に処理した SNMP 応答の残骸がメモリ上から漏えいする脆弱性です。攻撃に認証は不要であり、ネットワーク経由で SNMP リクエストを送信できる環境であれば誰でも悪用しうる点が大きな特徴です。

原因は、SNMP の OID（オブジェクト識別子）を BER 仕様上有効な冗長バイト（0x80 など）で水増しして送信した際、mini-snmpd 内部で OID の長さ計算・応答バッファの確保・実際の書き込みサイズとの間に不整合が生じることにあります。

この結果、確保された領域のうち実際にデータが書き込まれない部分が初期化されないまま応答に含まれ、外部に送出されてしまいます。

■発見の経緯

この不整合は、通常の SNMP クライアントが送信しないような「冗長エンコードされた OID」を入力として初めて表面化するものであり、一般的な機能テストや典型的な入力パターンの検証では検出が極めて困難です。We-Fuzz 社の検証チームは、Penzzer が備える、仕様上は許容されるものの実装上は想定されにくい境界値・異常系の入力パターンを高速かつ網羅的に生成・投入するファジング技術により、通常の検証プロセスでは発見が困難なこの種の脆弱性を的確に検出しました。

■想定される影響

漏えいする情報には Community String（public/private を含む独自設定の認証文字列）、システム名（sysName）、システム記述（sysDescr）などの MIB 情報、さらには、他の監視システムからの問い合わせ内容が含まれる可能性があります。とりわけ UDP で SNMP 通信を行う環境では、mini-snmpd が応答バッファを複数クライアントで共有する実装となっているため、ある管理者向けの応答が別の第三者に漏えいする可能性があり、注意が必要です。TCP 接続の場合は影響範囲が同一接続内の自己データに限定されると考えられますが、いずれの通信方式においても認証情報が外部に露出しうる点で看過できないリスクです。

なお、本脆弱性はデータの改ざん（完全性）やサービス停止（可用性）には影響しません。漏えいする範囲も SNMP バッファ内の最大 2,048 バイトに限られ、アドレス情報の漏えいや ASLR 回避への悪用にはつながらないため、任意のメモリ領域を大量に読み出せる「Heartbleed」とは深刻度・悪用範囲の両面で性質が異なります。一方で、認証情報である Community String が窃取されれば、そのまま該当ネットワーク機器への不正アクセスの足がかりとなり得ます。このため、CVSS v4 評価は High（両社による暫定評価）とされており、実運用環境においては早急な対応が推奨されます。

■対策

mini-snmpd の開発元は、本脆弱性を修正した mini-snmpd 2.1 をリリース済みです。修正版では、OID の長さを受信時の値ではなくデコード後に再計算した最小長で扱うよう変更されており、未初期化領域が発生する余地がなくなっています。mini-snmpd 2.0 以下を利用している組織には、速やかにバージョン 2.1 以降へアップデートすることを強く推奨します。

■脆弱性概要

- 脆弱性名：MIBleed
- CVE 番号：申請中
- 影響製品：mini-snmpd 2.0 以下
- 修正版：mini-snmpd 2.1
- 種類：未初期化メモリ情報漏えい（Uninitialized Memory Disclosure）
- 攻撃条件：ネットワーク経由での SNMP リクエスト送信のみ、認証不要
- 主な影響：Community String を含む過去の SNMP 応答内容の漏えい
- CVSS v4：High（両社による暫定評価）
- 発見者：We-Fuzz Inc.
- 発見ツール：ファジングツール「Penzzer」

■本発見が示すもの

MIBleed は、公開から長期間にわたり数多くの環境で稼働してきたソフトウェアであっても、実運用を模した網羅的なファジングによって未知の脆弱性が発見されうることを示す事例です。We-Fuzz 社は今後も Penzzer の技術開発を通じて、ソフトウェアサプライチェーン全体のセキュリティ品質向上に貢献してまいります。また、日本国内で Penzzer の提供と IoT デバイスセキュリティ検証サービスを手掛けるユビキタス AI は、本発見を一つの証左として、国内の製造業・IoT 関連事業者に向けた脆弱性検証支援を強化してまいります。

■Penzzer について

Penzzer は、近年深刻化する IoT 機器・組込みシステムへのサイバー攻撃に対応するために、米国 We-Fuzz Inc.が開発した、ファジングとペネトレーションテストを単一のユーザーインターフェースに統合したセキュリティ検証ツールです。従来の検証手法では発見が困難な未知の脆弱性（ゼロデイ脆弱性）の検出に強みを持ち、200 以上のプロトコルに対応します。日本国内ではユビキタス AI が正規提供元として、IoT デバイスセキュリティ検証サービスに Penzzer を活用し、製造業・医療機器・自動車・IoT・無線インフラなど、幅広い分野の製品セキュリティ強化を支援しています。

■We-Fuzz Inc.について

We-Fuzz Inc.は、IoT・車載・医療・産業システム向けのセキュリティテストに特化したサイバーセキュリティ企業です。従来分断されていたファジング（未知の脆弱性・ゼロデイ検出）と脆弱性スキャン（既知の脆弱性検出）とを統合することを目的に、2025年に設立されました。ミッションクリティカルな製品領域において、既知・未知の脆弱性を同時に効率よく検出し、ISO/SAE 21434、FDA、IEC 62443、CRAなどの規格や規制の対応におけるテストと証跡作成の両立を可能にするツールとして「Penzzzer」を開発しています。

URL：<https://www.we-fuzz.io/>

■株式会社ユビキタス AI（証券コード：3858）について

ユビキタス AI は、製造業のお客様を支えるテクノロジーとサービスを提供する企業です。長年にわたる組込みソフトウェアビジネスの実績をベースに、自社開発製品および世界中のソフトウェア製品の販売・サービスにおいて成功を収めています。強みである先進かつ優れたテクノロジーと強固で幅広い顧客基盤を活かしながら、製造業のお客様を支えるテクノロジー・サービスを世界に展開し続けることによって「お客様」「ビジネスパートナー」「社会」の発展に貢献します。

本社所在地：東京都新宿区西新宿 1-23-7 新宿ファーストウエスト 17F

URL：<https://www.ubiquitous-ai.com/>

■投資家の皆さまへ

本ニュースリリースは、ユビキタス AI の定性的な業務進捗をお知らせするためのものであり、投資勧誘を目的としたものではありません。当社業績・経営指標の進捗・予想に関しては、取引所開示情報である、決算短信などをご参照ください。

■本ニュースリリースに関するお問い合わせ先

株式会社ユビキタス AI マーケティング&コミュニケーション部（担当：麻生）

TEL：03-5908-3451

Web からのお問い合わせ：<https://www.ubiquitous-ai.com/contact/others/>

We-Fuzz Inc.に関するお問い合わせ：<https://www.we-fuzz.io/>

※ 本ニュースリリースに記載されている会社名、製品名は各社の登録商標または商標です。

※ 本ニュースリリースに記載された内容は発表日現在のものです。その後予告なしに変更されることがあります。