複数の脆弱性の組み合わせが新たな脅威となることも・・・

【事例】オープンソースのCMSソフトウェアで2種類の脆弱性が公開される。
1. ユーザーアカウント作成機能を制限しているにも関わらず作成できてしまう脆弱性
2. ユーザーアカウントの権限昇格の脆弱性

２つの脆弱性を組み合わせると自由に管理者アカウントが作成でき、この管理者アカウントが悪用されることで、CMSで管理しているWebサイトが乗っ取られる懸念があることから、リスクレベルの高い脅威となりました。実際に当時、多くの攻撃者によって悪用が試みられました。

サービス概要

専門のセキュリティ技術者により、実際のサイバー攻撃と同等の擬似攻撃を仕掛けることで、システム全体のセキュリティレベルを総合的に評価致します。

おもなテスト項目

1. 一般公開情報を調査し攻撃者において悪用可能な情報を探索
2. 脆弱性診断で顕在化した脆弱性を組み合わせたリスクの評価
3. 脆弱なパスワードの洗い出し
4. Exploitコードを利用したシステム侵入の試行
5. 脆弱性を悪用した権限昇格の試行
6. 不正侵入後の感染拡大、権限奪取の試行

実施内容

サービス内容		
サービス名	ペネトレーションテスト	
診断対象	IPアドレス・FQDN単位	
診断経路	リモートテスト・オンサイトテスト	
サービス内容	1．偵察（情報収集）	テスト対象システム及び周辺情報に関する公開情報の有無、攻撃者において悪用可能な有用情報の有無等を調査します。
	2．把握（脆弱性診断）	ネットワーク診断、Webアプリケーション診断を行い、対象システムに内在する脆弱性を調査します。
	3．攻撃シナリオの検討	脆弱性診断で発見された脆弱性や偵察で入手した情報を組み合わせることで、攻撃シナリオを検討し、そのリスク評価を行います。
	4．侵入検査（脆弱性悪用調査）	Exploitコードを利用したシステム侵入を試行し、脆弱性の悪用可否を調査します。また、脆弱なパスワードの洗い出しも行います。 ※本番系システムでの実施については事前に詳細ヒアリングを行います
	5．侵入後の影響調査 ※オプション	システム侵入が可能である場合、侵入後の感染拡大や権限奪取の可否を調査します。また、事前にアカウント情報の提供を受けた調査の実施も可能です。 ※本番系システムでの実施については事前に詳細ヒアリングを行います
	6．報告書・報告会 ※報告会はオプション	報告書の内容： ・偵察・把握フェーズでの調査結果 ・攻撃シナリオの内容 ・侵入検査結果 ・（影響調査結果） ・総合的なリスク評価と推奨対策 オプションの報告会は、弊社技術者がお客様先へご訪問し、対面にてリスクのご説明や必要対策の助言等を行います。
	7．QA対応	ペネトレーションテストの実施後1ヵ月間、報告書内容に関するお問い合わせへの対応を行います。
成果物	ペネトレーションテスト実施報告書	
価格	下記までお問い合わせください	

■お問い合わせ
ストーンビートセキュリティ株式会社
TEL：03-6869-9567　FAX：03-6869-6430
E-mail：sales@stonebeat.co.jp

Stonebeat Security
Your Trusted Security Advisor
www.stonebeat.co.jp