熊本大学公式 WEB システムセキュリティ監査支援

谷口勝紀，青木敏裕
先端情報グループ

1　はじめに

熊本大学公式 WEB システムは、データベースや LDAP 認証、PloneCMS システムなどの機能毎に分割/最適化されて構築されている。　これらのシステムは、ホストサーバ 2 台の上で仮想化されたサーバで 8 台、仮想化されていない WEB アクセス用サーバ 1 台の、合計 11 台のサーバ群で構築され、非常に厳格なルールでアクセス制限設定が施されており、内部のごく限られた端末からでしかアクセスできないよう制御されている。

本業務はマーケティング推進部広報戦略室依頼のもと、WEB システムへセキュリティ監査を行い、調査結果および脆弱性への対応法を報告している。

2　支援内容

ホストサーバ・GW サーバが仮に被害に遭った場合、その他のサーバ群へアクセス可能なルートができてしまう。

そこで、ホストサーバ・GW サーバが踏み台にされるという最悪の状況を想定し、これらのサーバから OpenVAS を用いて疑似攻撃を他のサーバへ行う事により、脆弱性の有無を確認する。　OpenVAS は 2017 年 3 月時点で、NVT フィードを用いて検証する脆弱性の数は 50,000 を超えている。

3　まとめ

例年職員の繁忙期や WEB 利用が多い時期を避け、4 か月に一回程度のセキュリティ監査を行っているが、震災の影響で本年は 2 回の実施となった。　実際に監査を行った期間は H28 年 9 月 6 日~7 日、H29 年 1 月 17 日~18 日である。

検出したアラートは CVE と呼ばれる脆弱性の種別を表したナンバーでレポートされるが、そのままでは意味をなさない。　脆弱性の内容を精査し、解析する事で対応するサービスを突き止め、より具体的な内容で報告書を作成する事で、脆弱性のアップデートが可能となる。

今回の支援では、OpenVAS の結果を精査した報告書の作成し、対処法などを報告する事で脆弱性を埋める作業に貢献することが出来た。

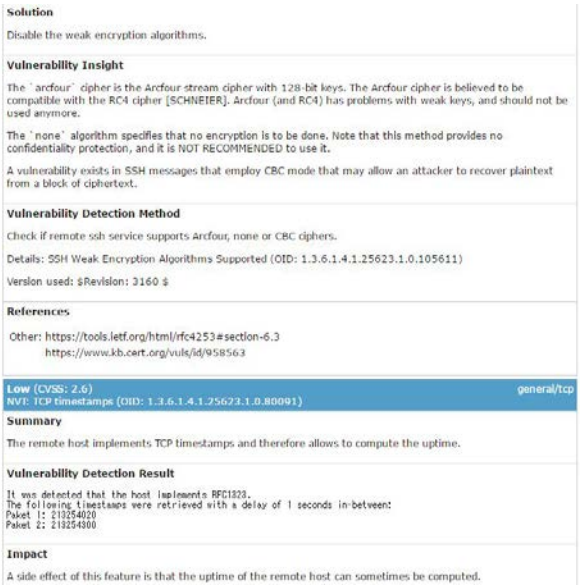

図 1. OpenVAS セキュリティ監査結果例

参考 URL：

熊本大学：http://www.kumamoto-u.ac.jp/

OpenVAS: http://www.openvas.org/