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
電気情報技術系

1　はじめに

熊本大学公式 WEB は、H23 年度末にリニューアルされ、新たなシステム上で稼働している。　新 WEB システムでは機能毎に分割/最適化されて構築されており、仮想化されたサーバで 8 台、ホストサーバ 2 台、仮想化されていない WEB アクセス用サーバ 1 台の、合計 10 台を超えるサーバ群で構築されている。　これらサーバは、アクセスは非常に厳しいルールで制限されており、内部の極めて限られたポイントからでしかアクセスされないよう制御されている。

本業務支援で行ったセキュリティ監査の範囲は、サーバシステムが持つセキュリティの脆弱性を検出する事にある。ここでいうセキュリティの脆弱性とは、OS やサービスプログラムが持つ脆弱性に止まらず、設定方法等の面からも含んでいる。

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 サーバが乗っ取られた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 2012 年 5 月時点で、NVT フィードを用いて検証する脆弱性の数は 25,000 を超えている。

3　まとめ

職員の繁忙期や WEB 利用が多い時期を避け、4 半期に一回程度のセキュリティ監査を行った。

H25 年 7 月 9 日~10 日、H24 年 10 月 2 日~4 日、H25 年 1 月 8 日~10 日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、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まで行い、脆弱性を埋める作業に貢献することが出来た。

参考 URL：http://www.kumamoto-u.ac.jp/

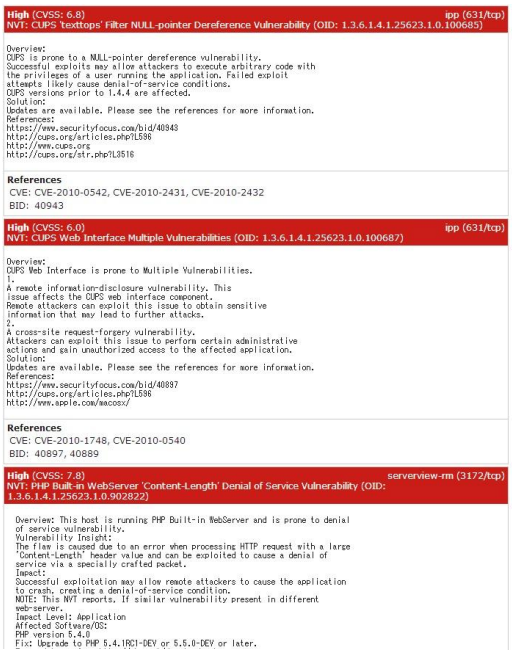

図 1．OpenVAS セキュリティ監査結果例