

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/>

| |
|---|
| High (CVSS: 6.8) NVT: CUPS 'texttops' Filter NULL-pointer Dereference Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.100685) ipp (631/tcp) |
| Overview: CUPS is prone to a NULL-pointer dereference vulnerability. Successful exploits may allow attackers to execute arbitrary code with the privileges of a user running the application. Failed exploit attempts likely cause denial-of-service conditions. CUPS versions prior to 1.4.4 are affected. Solution: Updates are available. Please see the references for more information. References: https://www.securifyinc.com/blog/40845 http://cups.org/articles.php?L588 http://www.cups.org https://cups.org/str.php?L5816 |
| References CVE: CVE-2010-0542, CVE-2010-2431, CVE-2010-2432 BID: 40943 |
| High (CVSS: 6.0) NVT: CUPS Web Interface Multiple Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.100687) ipp (631/tcp) |
| Overview: CUPS Web Interface is prone to Multiple Vulnerabilities. 1. A remote information-disclosure vulnerability. This issue affects the CUPS web interface component. Remote attackers can exploit this issue to obtain sensitive information that may lead to further attacks. 2. A cross-site request-forgery vulnerability. Attackers can exploit this issue to perform certain administrative actions and gain unauthorized access to the affected application. Solution: Updates are available. Please see the references for more information. References: https://www.securifyinc.com/blog/40897 http://cups.org/articles.php?L588 http://www.apole.com/wacoss/ |
| References CVE: CVE-2010-1748, CVE-2010-0540 BID: 40897, 40889 |
| High (CVSS: 7.8) NVT: PHP Built-in WebServer 'Content-Length' Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902822) serverview-rtm (3172/tcp) |
| Overview: This host is running PHP Built-in WebServer and is prone to denial of service vulnerability. Vulnerability Insight: The flaw is caused due to an error when processing HTTP request with a large Content-Length header value and can be exploited to cause a denial of service via a specially crafted packet. Impact: Successful exploitation may allow remote attackers to cause the application to crash, creating a denial-of-service condition. NOTE: This NVT reports, if similar vulnerability present in different web-server. Impact Level: Application Affected Software/OS: PHP version 5.4.0 Fix: Upgrade to PHP 5.4.1(RC1)-DEV or 5.5.0-DEV or later. |

図 1. OpenVAS セキュリティ監査結果例