February 11, 2013

In this edition we cover five CRITICAL threats that local organisations need to address. Pay extra attention to the Joomla and UPnP vulnerabilities as this could be a big headache considering the number of local organisations running Joomla websites. Also remember to look at the New PCI Guidelines especially for institutions that are launching online portals or customer facing web applications..

Contents

CRITICAL: Multiple Vulnerabilities in Cisco Wireless LAN Controllers

Discovery: Cisco recently released a FREE software updates for the multiple vulnerabilities affecting Cisco Wireless LAN Controller (Cisco WLC) product family. The Cisco WLC is responsible for system-wide wireless LAN functionality, including security policies, intrusion prevention among others

These vulnerabilities include:

- **Cisco Wireless LAN Controllers Wireless Intrusion Prevention System (wIPS) Denial of Service Vulnerability**

  This vulnerability could allow an unauthenticated, remote attacker to cause the device to reload by sending crafted IP packets to the affected device. This vulnerability affects Cisco WLCs that are configured with Wireless Intrusion Prevention System (wIPS). This vulnerability can be exploited from both wired and wireless segments.

- **Cisco Wireless LAN Controllers Session Initiation Protocol Denial of Service Vulnerability**

  This DoS vulnerability exists on the Cisco Wireless Access Points(AP) that are managed by Cisco Wireless LAN Controllers (WLC) which could allow an unauthenticated, remote attacker to cause the AP to reload by sending crafted Session Initiation Protocol (SIP) packets to the affected device. This vulnerability can be exploited from both wired and wireless segments. This vulnerability can be triggered by transit traffic and even if SIP features are disabled on the device.

- **Cisco Wireless LAN Controllers HTTP Profiling Remote Code Execution Vulnerability**

  If the HTTP profiling feature in these devices is enabled, then the device is vulnerable and allows an unauthenticated, remote attacker to execute arbitrary code on an affected device by sending a crafted UserAgent string. This vulnerability can be exploited from both wired and wireless segments

  You can check whether your HTTP profiling feature is enabled or not by issuing the show **wlan** command

- **Cisco Wireless LAN Controllers SNMP Unauthorized Access Vulnerability**

An unauthenticated attacker could view and modify the configuration of an affected Cisco WLC via SNMP **even if "management over wireless" feature is disabled.**

Affected Systems: The Cisco WLC product family is affected by at least one of the vulnerabilities mentioned above.

Exploitation: Successful exploitation of the DoS vulnerabilities could allow an unauthenticated attacker to cause an affected device to reload. Repeated exploitation could result in a sustained DoS condition.

Successful exploitation of the HTTP Profiling Remote Code Execution Vulnerability could allow an authenticated, remote attacker to perform remote code execution on the affected device.

Successful exploitation of the unauthorized access vulnerability could allow an unauthenticated attacker to view or modify the device configuration even if "management over wireless" is disabled.

Mitigation: It is essential that all Cisco WLC product customers update their devices with the software updates released by Cisco. Workarounds that mitigate these vulnerabilities are available**.** See link http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130123-wlc

Visit this link to determine exposure and a complete upgrade solution http://www.cisco.com/go/psirt

More Information: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130123-wlc

CRITICAL: JOOMLA (Content Management System) SQL Injection and Cross-Site Scripting Vulnerabilities

Discovery: Security experts revealed multiple cross-site scripting and SQL injection vulnerabilities in the 'Do-It-Yourself' –Content Management System (DIY CMS) version 1.0 used in the development of mostweb applications and websites. These vulnerabilities allow cyber criminals to inject client-side script (JavaScript, VBScript, ActiveX, HTML, or Flash) into webpages viewed by other users. This means that attackers introduce malicious code into a computer program to change the course of execution and collect sensitive data from the victim such as access credentials, credit card numbers, manipulate or steal cookies etc.

Affected Systems: All dynamic websites developed on CMS version 1.0. The most commonly used DIY CMS tools include Joomla and Drupal.

Exploitation: Attackers exploit cross site-scripting (frequently referred to as CSS or XSS) vulnerability by carefully crafting a URL to execute script in a victim's web browser, this allows them to steal user accounts, conduct phishing attacks and client-side content request manipulation. This attack is normally perpetrated through the *add.php* and *edit.php* script found in the Content Management System.

The SQL Injection vulnerability is exploited by the attacker by executing their own SQL commands on the affected application Database Management System (DBMS). This results in DBMS and application compromise of its confidentiality and integrity.

Mitigation: Unfortunately, there are no known workarounds or vendor patches available. And subsequently, no remedy available as of February 1, 2013. However, Vulnerability Lab has released an unofficial patch to help address this vulnerability. As with all third-party solutions, before downloading a patch and installing it, ensure they come from a reliable source and are permitted under your company's security policy. In addition, common vulnerabilities such as the SQL Injection can be addressed by applying simple but prudent coding practices in the organization; whether the system is developed in-house or by a third party. Serianu recommends the following sources for secure coding practices:

- Open Web Application Security Project (OWASP)
- SANS
- CERT/CC – CERT Coordination Centre
- Information Systems Audit and Control Organization (ISACA)

More information: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6517

CRITICAL: New PCI Guidelines released for E-Commerce

PCI Security Standards Council has written and released a new document to help E-commerce companies understand and conform to the requirements of the PCI Data Security Standard with particular reference to hybrid infrastructures including software from third parties. The document, *PCI DSS E-commerce Guidelines* was released last week, January 31st.

This document is a guideline and not an official extension of PCI DSS. It however gives an overview of the e-commerce infrastructure, its relevance to PCI DSS, common vulnerabilities in the e-commerce environment together with recommendations on how to overcome them and also provides guidance on the necessary steps organizations using the card-not-present environment should conform to when it comes to PCI DSS.

Key takeaways from this document include:

- Securing the Payment Chain: The guideline offers a checklist of security recommendations and reminders such as:
  - Evaluate risks associated within e-commerce technology.
  - Review the network and database risks posed by outsourcing functions, such as payments processing and Web hosting to third parties.
  - Hire PCI-approved website scanning vendors to validate, on a regular basis, Internet-facing environments for compliance with the PCI Data Security Standard.
  - Define best practices for online payment application security.
  - Ensure that vendors are regularly assessed and scanned for vulnerabilities to their networks.
  - Ensure that any agreements you have with third parties who handle cardholder data clearly line out who is doing what, who is responsible for what, and how disputes are handled.

This document is essential to all organizations that allow their consumers to make payments online. We **STRONGLY** recommend that the guidelines are read and understood in order to comply with the PCI DSS standards.

CRITICAL: Google Finds 86000 HP Printers Open to Hack via port3000

Discovery

It has been revealed that more than 86000 publicly available HP printers can easily be hacked through Google hack. A hacker could use a quick well-crafted Google Search script to access any of these printers and send unwanted commands to the printer, for example, printing of paper! With the simple script, hackers can remotely bypass the printers' passwords to access and use the machine. The unfortunate thing though is that many of these printing devices either have no password at all or use the default HP passwords.

Those printers are often used as public devices, such as in the university, which as a result put the whole organization at risk of exposure.

Affected Systems: Publicly available HP printers

Exploitation: According to the report, people can use a simple Google Dork search with the following address to easily find these Google indexed printers: inurl:hp/device/this.LCDispatcher?nav=hp.Print.

Hackers can control and manage these unprotected network-enabled printers, gaining details like the level of ink or toner in their HP printer cartridges, the number of pages it had printed, and the titles of these documents.

Mitigation: There are security concerns here, as many printer models have known exploits which can be used as an entry point to a private network. Consumers of these devices are advised to ensure that their printers are not exposed to the internet through port 3000; this means that they can be directly accessed from outside the company's firewall.

Hewlett-Packard, in an official statement encouraged its customers to protect their printers by placing firewalls, passwords and providing network credentials only to their trusted parties. *"By following the HP recommended security features, printers should not be accessible to the public via the internet."*

More Information: http://www.cloudave.com/25618/new-hp-printer-google-hack-via-port3000/

CRITICAL: Oracle JAVA SE Patch Release Update Advisory

Oracle has published a major security update for Java. The update was originally scheduled for February 19th, but was released a fortnight early on Friday because of "active exploitation 'in the wild' of one of the vulnerabilities affecting the Java Runtime Environment (JRE) in desktop browsers". Customers are **STRONGLY** advised to apply the fixes as soon as possible.

According to the latest Oracle Risk Matrix, the update covers a total of 50 flaws: 49 of these can be remotely exploited - in other words just visiting a web page, for instance, might be enough to infect your computer; 26 carry the maximum Common Vulnerability Scoring System (CVSS) risk score of 10. Oracle hasn't said which of the remote code execution holes is the one that's actively being exploited but it is addressed with this patch.

Affected Systems: JDK and JRE 7 Update 11 and earlier

- JDK and JRE 6 Update 38 and earlier
- JDK and JRE 5.0 Update 38 and earlier
- SDK and JRE 1.4.2_40 and earlier
- JavaFX 2.2.4 and earlier

Visit link http://www.oracle.com/technetwork/topics/security/alerts-086861.html for information about Oracle Security Advisories.

Portable SDK for Universal Plug and Play (UPnP) Devices (libupnp) contains multiple buffer- overflows in SSDP (Simple Service Discovery Protocol)

Discovery: About a week ago, as part of a large scale security research project security consultants investigated internet-connected UPnP devices and found, among other security issues, multiple buffer overflow vulnerabilities in the libupnp implementation of the Simple Service Discovery Protocol (SSDP).

UPnP is a set of network protocols designed to support automatic discovery and service configuration. It enables easy communication between computers and network-enabled devices.

The libupnp is vulnerable to multiple stack-based buffer overflows when handling malicious SSDP requests. Out of the tens of millions of network devices (e.g. routers, printers, network-attached storage, smart TV, media player) that utilize libupnp, 20 million are exposed directly to the internet.

Affected Systems: Hundreds of vendors that use libupnp in their products have confirmed to have been affected by the buffer overflow vulnerabilities. This includes CISCO systems, D-Link Systems, Linksys, and Fujitsu Technology among others. Some may have however updated the flaw from the time they were notified.

Exploitation: A remote, unauthenticated attacker may be able to execute arbitrary code on the device or cause a denial of service attack to users who use these systems as home routers for consumer network.

Mitigation: If you are using the library in your devices, ensure that you update using the recently released patch, libupnp1.6.18, to address these vulnerabilities. Secondly, deploy firewall rules to restrict untrusted hosts from being able to access port 1900/udp (This UDP port is opened and used by Universal Plug N' Play (UPnP) devices to receive broadcasted messages from other UPnP devices). Finally, consider disabling UPnP on the device if it is not absolutely necessary especially if it has been configured on external facing systems and devices providing critical information.

More information: **http://www.kb.cert.org/vuls/id/922681**

About the Serianu Cyber Threat Alert Service

For more detailed and customized vulnerability management service, e-mail us at info@serianu.com