January 14, 2013

During the past week there has been a lot of activity and concern around vulnerabilities in three different widely used technologies: Java, Ruby on Rails and Cisco VOIP Phone. With this Alert, we would to help you understand the situation, the risks, and provide you with information on how you can protect your ICT environment. In this edition we cover three **EXTREMELY CRITICAL** threats that you need address urgently.

Contents

1. Deadly Java Vulnerability Leaves PCs Open To Hackers
2. Extremely critical Ruby on Rails bug threatens more than 200,000 sites
3. Cisco VOIP phone exploit allows attackers to listen in on phone calls
4. Oracle to release security patches for MySQL, E-Business Suite and JD Edwards etc.

CRITICAL: Deadly Java Vulnerability Leaves PCs Open to Hackers

Discovery: Last week, cyber security researchers identified a very serious weakness in Java. The Java vulnerability situation is critical since it is a zero day vulnerability, which means there is no patch available from Oracle at this time. Unfortunately, cyber criminals have figured out how to use this weakness to access computer networks (business and home networks) without the need for a username and password. This allows the cyber criminals to install malicious software (e.g. Keyloggers) enabling them to commit crimes ranging from identity theft to making an infected computer part of an ad-hoc network of computers that can be used to attack websites. To successfully exploit the Java weakness, an unsuspecting user running an affected release in a browser will need to visit a malicious web page that leverages this vulnerability. Successful exploits can impact the availability, integrity, and confidentiality of the user's system or company network.

Affected Systems: Java Version 1.7.10 SDK – All browsers that require the Java SDK plugin (Majority of enterprise applications in banks, insurance companies and major organisations)

Exploitation: The vulnerability can be exploited when a user unknowingly visits one of the millions of compromised website (either by clicking on an email link). The request to the website is redirected from the initial infected website server to the server hosting the malware. The infected server infects the user's computer with malware (KeyLoggers or other malicious software). If the exploit is successful, the cybercriminals will install malicious software enabling them to commit crimes ranging from identity theft to making an infected computer part of an ad-hoc network of computers that can be used to attack websites.

Mitigation: Early this morning, Oracle released a software update to fix a critical security vulnerability in its Java software that miscreants and malware have been exploiting to break into vulnerable computers. javanix2Java 7 Update 11 fixes a critical flaw (CVE-2013-0422) in Java 7 Update 10 and earlier versions of Java 7. The update is available via Oracle's Web site, or can be downloaded from with Java via the Java Control Panel. Existing users should be able to update by visiting the Windows Control Panel and clicking the Java icon, or by searching for "Java" and clicking the "Update Now" button from the Update tab.

Download Oracle Patch: http://www.oracle.com/technetwork/java/javase/downloads/index.html

Serianu Java Zero Day Remediation Service

To assist local organisations address the problem – Serianu is offering a short-term service to detect and remediate against the vulnerability, especially for organisations that rely on applications that require their users to use Java applets and Java plugin supported systems. Serianu will work with the ICT team to remediate all the affected user desktops.

Key steps every organisation should follow to limit Malware infection.

- Configure their firewalls and network security devices and disallow access to non-intranet resources.
- Allow business users to use two browsers, one to access the web and the other to only access the internal applications. The browser accessing the external websites should have Java disabled while the alternate can keep Java but should be closely monitored.
- Ensure that ICT systems limit internet access to suspicious websites.
- Advise users to avoid clicking on any suspicious links or emails.
- Institute log monitoring and reviews to ensure any outgoing traffic is not targeting suspicious servers.

For more details on the vulnerability and instructions on how to disable Java use the links provided below.

- Oracle Java 7 Security Manager Bypass Vulnerability: http://www.us-cert.gov/cas/techalerts/TA13-010A.html
- How to Disable Java on your computer/browser: http://www.oracle.com/technetwork/java/javase/downloads/index.html

CRITICAL: Critical Ruby on Rails vulnerability threatens more than 200,000 sites

Discovery: A recently discovered vulnerability in Ruby on Rails (a popular web development framework used in the development of Web and Mobile applications) puts thousands of websites at risk of being hacked. This vulnerability is critical and given the popularity of Ruby on Rails, the impact is huge. In Kenya, there are several websites belonging to large organisations and thousands of smaller businesses and private organisation that are developed using Ruby on Rails. Globally various major organisations are using Ruby on Rails, including Twitter, Groupon and Github.

Affected Systems: All Rails versions prior to those released on January 8, 2013 are vulnerable.

Exploitation: Anyone who is able to make HTTPs request to your Rails application can exploit the vulnerability. No special knowledge of the application is required to test it for the vulnerability, making it simple to perform automated spray-and-pray scans. Attackers can execute shell code at the privilege level of the application process, potentially leading to host takeover. This means all of your data could be stolen and your server resources could be used for malicious purposes.

Mitigation: Local organisations need to reach out to their web application and mobile solution providers and find out if any of their applications were developed using Ruby on Rails Framework. If this is confirmed - organisations that use Ruby on Rails in their applications and have not disabled XML parsing, should update to versions 3.2.11, 3.1.10, 3.0.19, or 2.3.15 as soon as possible as the risk of compromise has escalated with deadly exploits and Proof of concepts coming out.

More information:
http://weblog.rubyonrails.org/2013/1/8/Rails-3-2-11-3-1-10-3-0-19-and-2-3-15-have-been-released/

Cisco VOIP Phone vulnerability allows attackers to remotely eavesdrop in on phone calls

Discovery: Last week Cisco released a security advisory of vulnerability in its VOIP phones that could potentially allow an attacker to eavesdrop on phone calls and conversations. Cisco's VoIP devices are used worldwide by many enterprises including major corporations, banks and governments.

Affected Systems: Cisco Unified IP Phones 7900 Series, also known as TNP phones.

Exploitation: The attack can be carried out by gaining local access via the AUX port located on the rear of the device or remotely by authenticating to the device via SSH and executing malicious code. The phone can be tricked into turning the microphone on while the handset is still on the hook.

Mitigation: Cisco released a partial patch to address the vulnerability but the patch does not fully remediate the patch. Cisco is currently working on a long-term remediation of the core vulnerability. Over the next several months, Cisco will be rewriting portions of the 7900 series firmware to fully mitigate the underlying root cause to improve both the network and physical security posture of the affected devices.

More information:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130109-uipphone

Oracle to release product security patches including (MySQL, E-Business Suite and JD Edwards)

If you an Oracle customer, you need to look out for the upcoming patch release. This week Oracle will release their quarterly Critical Patch Update. In this update, oracle is releasing fixes for security vulnerabilities across most of its enterprise products, addressing a host of remotely exploitable flaws. Oracle Financial Services Software's FLEXCUBE Direct Banking and FLEXCUBE Universal Banking are also vulnerable to a remote exploit. Oracle also reports 11 patches for its PeopleSoft and Siebel CRM products (. There is a remotely exploitable vulnerability being repaired for each. Two remotely exploitable vulnerabilities are being exploited in MySQL Server; 14 in total. Here is a list of patches you need to look out for:

- Oracle VM Virtual Box, versions 4.0, 4.1, 4.2
- Oracle MySQL Server, versions 5.1.66 and earlier, 5.5.28 and earlier
- Oracle PeopleSoft HRMS, versions 9.0, 9.1
- Oracle PeopleSoft PeopleTools, versions 8.51, 8.52
- Oracle WebLogic Server, versions 9.2.4, 10.0.2, 10.3.5, 10.3.6, 12.1.1
- Oracle Database 11g Release 2, versions 11.2.0.2, 11.2.0.3
- Oracle Database 11g Release 1, version 11.1.0.7

Serianu recommends that you establish vulnerability and patch management program that enables you to continuously detect and remediation software vulnerabilities.

About the Serianu Cyber Threat Alert Service
For more detailed and customized vulnerability management service, email us at info@serianu.com