In this edition we cover two threats that local organisations need to address. Pay extra attention to the Java based malware as this could be a big headache considering the number of local organisations running java application servers in their environment.

Contents

Microsoft Internet Explorer 6, 7, 8 Zero Day Vulnerability

Discovery: Last week a number of security firms reported that hackers had exploited the zero-day bug in Internet Explorer to compromise a number of websites. The websites were compromised with JavaScript that served malicious code to older IE browsers and the code then created a heap-spray attack using Adobe Flash Player.

Affected Systems: Microsoft Internet Explorer version 6, 7 and 8

Exploitation: The vulnerability can be exploited by manipulating a website in order to attack vulnerable browsers with one of the most dangerous types of attacks known as a drive-by download. Victims merely need to visit the tampered site in order for their computer to become infected. To be successful, the hacker would have to lure the person to the harmful website, which is usually done by sending a malicious link via email.

Mitigation: Microsoft has published a security advisory warning users of Internet Explorer 6, 7, and 8 that they could be vulnerable to remote code execution hacks. These vulnerabilities could allow an attacker to bypass security features or remotely execute arbitrary code.

Microsoft has provided a "Fix it" solution designed to reduce the attack surface of this vulnerability. This code-signed, one-click deployable Microsoft “Fix it” package uses the Windows application compatibility toolkit to make a small change at runtime to mshtml.dll every time Internet Explorer is loaded. For enterprise deployment, please refer to Knowledge Base article 2794220, section “Deploying an application compatibility database across multiple computers”.

More information: http://support.microsoft.com/kb/2794220

Malicious Software Targeting Java-based HTTP Servers

Discovery: Security researchers from antivirus vendor Trend Micro have uncovered malicious software that infects Java-based HTTP servers and allows attackers to execute malicious commands on the underlying systems. The malicious threat comes in the form of a Java Server Page (JSP), a type of Web page that can only be deployed and served from a specialized Web server with a Java servlet container. Once this page is deployed, the attacker can access it remotely and can use its functions to browse, upload, edit, delete, download or copy files from the infected system using a Web console interface.

Affected Systems: Systems running Windows 2000, Windows Server 2003, Windows XP, Windows Vista and Windows 7

Exploitation: For this attack to be successful, the targeted system must be a Java Servlet container (such as Apache Tomcat) or a Java-based HTTP server. Another possible attack scenario is when an attacker checks for websites powered by Apache Tomcat then attempts to access the Tomcat Web Application Manager.Using a password cracking tool, cyber criminals are able to login and gain manager/administrative rights allowing the deployment of Web application archive (WAR) files packaged with the backdoor to the server. The backdoor will be automatically added in the accessible Java Server pages.

Mitigation: In order to protect your systems from this threat, you should use strong passwords that cannot be easily cracked by using brute force tools, should deploy all security updates available for your systems and software and should educate employees to avoid visiting unknown and untrusted websites.

More information: http://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-disguised-as-java-server-page-targets-web-hosting-servers/

Serianu encourages enterprise users and administrators to review the Fix-It solution and follow best-practice security policies to determine which updates should be applied.

Other related vulnerabilities

- **Multiple vulnerabilities in Apache HTTP server - https://blogs.oracle.com/sunsecurity/entry/multiple_vulnerabilities_in_apache_http2**
- **Remote code execution vulnerability in Hyperion Financial Management https://blogs.oracle.com/sunsecurity/entry/cve_2012_1714_tlist_6**
- **IBM Tivoli Storage Manager for Space Management unauthorized access http://xforce.iss.net/xforce/xfdb/80668**

About the Serianu Cyber Threat Alert Service

The Serianu Cyber-threat Alert Service informs local enterprises of the latest threats and vulnerabilities. These include; Botnets, Denial of Service (DoS), Hacking, Key Stroke Logging, Malware, software vulnerabilities and Phishing. We monitor a wide variety of Internet sources for reports of new vulnerabilities in Internet software, hardware, and/or services. We provide our customers with a timely and reliable source for vulnerability notification. We havea dedicated research team and a testing environment to validate new vulnerabilities that we collate and consolidate from a variety of sources. Please note in this alert we only share known vulnerabilities that could be exploited with the potential for significant damage or disruption is high.

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