MSP1 | Cyber Security Solutions & Services

Runtime Application Self Protection

What Is Runtime Application Self-Protection (RASP)?

Runtime application self-protection (RASP) is a security technology that is built into an application and can detect and then prevent real-time application attacks. RASP prevents attacks by "self-protecting" or reconfiguring automatically without human intervention in response to certain conditions (threats, faults, etc.).

RASP comes into play when the application is executed (runtime), causing the program to monitor itself and detect malicious input and behaviour. In real time, RASP analyzes both the application's behavior and the context of the behavior. Thus, continuous security analysis is implemented, with the system responding immediately to any recognized attacks.

RASP basically embeds security into the running application where it resides on the server. It then intercepts all calls to the system to ensure they're secure. Ultimately, RASP implants validation of data requests directly into the application.

RASP can be applied to Web and non-Web applications and doesn't affect the application design. Rather, the detection and protection features are added to the servers an application runs on. Currently, RASP technology exists for Java virtual machine and .NET Common Language Runtime.

Firewalls vs. RASP

Like RASP, firewalls inspect traffic and content and make decisions to terminate sessions. However, unlike RASP, perimeter firewalls can't see how traffic is being processed in applications. In addition, with mobile devices and cloud services proliferating, the perimeter is no longer clearly defined, making perimeter firewalls less effective.

Challenges for any CIO:

- Precision Application Protection
- Virtual Patching and version upgrade
- Pre-emptive Security or Zero Day attacks
- Version upgrades: Most applications are on older versions and hence very vulnerable.
- 100% Guaranteed security

Case study:

A new "severe" rated vulnerability (CVE-2017-9791) in the popular Apache Struts 2 Framework was reported on Friday, July 7, 2017. Within hours of the vulnerability's disclosure, several public proof-of-concept exploits [1] [2] became available that make the exploitation easy to execute.

Background

According to the Struts 2 Security Bulletin (S2-048) and an official Apache Struts announcement, it is possible to perform arbitrary Remote Code Execution attacks by specially crafted HTTP requests when using the Struts 2 Struts 1 plugin. Note that applications using Struts 2.5.0 and above are not affected by this vulnerability. As of this time, Apache has not published a public patch for the affected versions of Struts and recommends developers refactor their code.

Action Required

Waratek customers are protected against Code Injection and RCE attacks by the Waratek Application Security Platform's standard protections such as Process Forking, Reflection Abuse, Name Space Layout Randomization (NSLR) and Component Privilege De-escalation features. These features provide active and accurate protection against RCE attacks with minimal configuration and no tuning, eliminating the need to immediately address vulnerable Struts 2 code.

MSP1 Cyber Security Solutions & Services

Authorized Waratek Distributor

MSP1 helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, we enable businesses to transform the way they manage their information security and compliance programs.

With automation, tools and intelligence, we find better ways for businesses to overcome their security challenges. Our qualified security assessors, ethical hackers and other experts are some of the industry's most trusted sources for risk assessments, threat research, forensic investigations, and security training.

North America
46721 Fremont Blvd,
Fremont, CA 94538
United States
+1 (408) 769 5030
https://msp1services.com

India
11/11 Kamdhenu, Hariom
Nagar, Mulund East
Mumbai 400081, India
+ 91 9769757668