Critical error on Apache Struts2 allows hackers to take over the web server

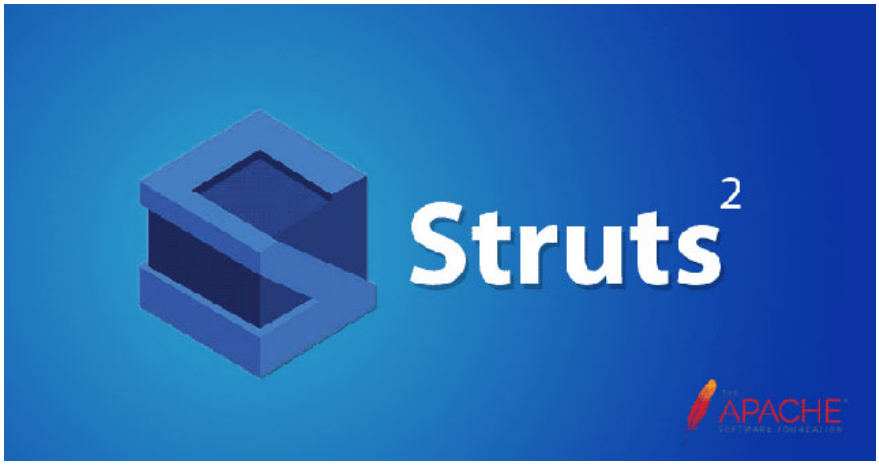
New researchers have discovered a remote code execution flaw in the Apache Struts open source web application framework, allowing an attacker to run malicious code on the server.

New researchers have discovered a remote code execution flaw in the Apache Struts open source web application framework, allowing an attacker to run malicious code on the server.

Apache Struts is a free open source Model-View-Control framework (MVC) for web application development written in Java, supporting both REST, AJAX and JSON.

This vulnerability (CVE-2017-9805) is a programming error in the way Struts handles data from unreliable sources. Specifically, Struts' REST plugin cannot handle XML payloads while converting data structures (deserialization) properly.

All versions of Apache Struts from 2008 (from Struts 2.5 to Struts 2.5.23) are affected, causing the framework's web applications to use REST plugins to be vulnerable to remote attacks.



The vulnerability on Apache Struts2 allows hackers to execute malicious code remotely

According to researchers at LGTM, the Struts framework is used by many organizations, including Lockheed Martin, Vodafone, Virgin Atlantic and IRS. 'Not to mention, the vulnerability is also very easy to use, all you need is a web browser,' said Man Yue Mo, researcher at LGTM. The attacker only needs to include the malicious XML code in a separate format to exploit this vulnerability on the server.

Successful exploits will allow hackers to take control of the entire infected server, thereby entering other systems on the same network.

Mo said that this error is due to the conversion of insecure data structures, similar vulnerabilities on Apache Commons Collections were discovered by Chris Frohoff and Gabriel Lawrence in 2015, also allowing the execution of random code.

Many Java applications have been affected by similar vulnerabilities in recent years. This vulnerability has been fixed from Struts 2.5.13 so administrators should update the Apache Struts they are using.