blackfoot Newsflash

ADVISE >
ASSESS >
ASSURE >

Apache Struts critical remote code execution vulnerabilities

Apache Struts 2 is an open source web framework for creating Java web applications. It is commonly used for retail websites, and if you use it for your website please take note.

We are aware that details of **6 critial Apache Struts v2 vulnerabilities** have been released since the 10th July.

The vulnerabilities work by exploiting various flaws in the input validation of URLs subsequently used by **Object-Graph Navigation Language (OGNL)**. They allow remote command execution, server context manipulation and injection of malicious client side code.

In one instance we are aware of this was used to allow an attacker to install a perl script malware and attempt to send a database dump to themselves. The target database was believed to hold customer details including name, email address and payment information. In this case the data was encrypted and with no keys available the data remained unusable. This is likely to have required a concerted effort from a coordinated group of hackers, however published exploits for these vunlerbabilities are appearing and this makes exploitation trivial.

If you or your third parties use a Struts 2 framework please ensure you are using the latest version, which is 2.3.15.1 as soon as possible. As this is a vulnerability being actively exploited now, please call us immediately if you have any questions.

Information about Struts can be found on the Apache Software Foundation website at **http://struts.apache.org/index.html**

Details of all vulnerabilities and patches can be found on the National Vulnerability Database run by NIST and the US Department of Homeland Security at **http://nvd.nist.gov/home.cfm**.