



## PRESS RELEASE

### VULNERABILITIES DISCOVERED IN ADOBE FLASH PLAYER PLUGIN ALLOW POTENTIAL ATTACKERS TO SEND ARBITRARY HTTP REQUESTS FROM USERS' BROWSERS, WARNS VULNERABILITY MANAGEMENT COMPANY RAPID7

*Rapid7 Reports Two Adobe Flash Vulnerabilities That Can Be Exploited with Specific Browser/Operating System Combinations and Potentially Used to Perform Cross-Site Request Forgery (CSRF) Attacks*

**BOSTON – October 17, 2006** – Two vulnerabilities found in Adobe Flash Player provide opportunity to attackers to send arbitrary HTTP requests from an unsuspecting user's browser, reports Rapid7 LLC in a security advisory published today (see <http://www.rapid7.com/advisories/R7-0026.jsp>). These vulnerabilities could be used in concert with cross-site request forgery (CSRF) vulnerabilities to steal cookies or other private information. Adobe Flash Player version 9.0.16 for Windows and version 7.0.63 for Linux, as well as earlier versions, are affected.

The exploits can be carried out through the vulnerabilities when Flash is used with the following browser/operating system combinations:

- Internet Explorer (IE) 6 Service Pack 2 (IE 6, Security Version 1) for Windows (with Flash 9.0.16)
- Firefox 1.5.0.6 for Windows (with Flash 9.0.16)
- Firefox 1.5.0.6 for Linux (with Flash 7.0.63)


The two vulnerabilities reported are as follows:

#### **XML.ADDREQUESTHEADER() VULNERABILITY**

The `addRequestHeader()` method insufficiently secures itself, providing a way around a security restriction that does not permit developers to use `addRequestHeader()` to set headers such as Host, Referer or Content-Length. As a result, it is possible to inject arbitrary headers with HTTP requests. The Rapid7 security paper points out that this vulnerability is similar to other, previously-reported vulnerabilities in Adobe Flash 7 and 8.

#### **XML.CONTENTTYPE VULNERABILITY**

The `XML.contentType` attribute contains the same vulnerability found in the `addRequestHeader()` and it can be exploited in the same way because Adobe Flash does not check the validity of the attribute's value before building the HTTP request.



According to Rapid7, Adobe was notified of the vulnerabilities but has not yet released a fix or upgrade to Adobe Flash Player. To protect from the risk of attack, Rapid7 offers four solutions in the interim:

- Upgrade to the beta version (Flash Player 9.0.18d60 for Windows), which is fixed;
- Only allow trusted Websites to use Flash;
- Use alternative Flash Plugins (GplFlash, Gnash); or
- Uninstall Adobe Flash Player.

According to Adobe, there are 700 million Adobe Flash users worldwide (source: labs.adobe.com).

To protect its customers, Rapid7 has added data on these two vulnerabilities to security checks performed by NeXpose, its enterprise network vulnerability management solution.

### **ABOUT NEXPOSE**

The award-winning NeXpose enterprise vulnerability management solution scans Web server applications, databases, operating systems, and network devices to locate threats, assess their risk to the environment, devise a remediation plan and implement the ticketing process. NeXpose incorporates an expert system to build a knowledge base of facts on the environment it explores and model potential targeted attacks to expose all existing threats. NeXpose provides robust reporting capabilities that ensure compliance with governmental regulations, corporate security configuration policies, and the PCI Data Security Standard.

### **ABOUT RAPID7**

Rapid7 was founded in 1999 by a team of software industry veterans who were major contributors to product development and subsequent growth and success at Percussion Software, Bond Technologies and Stride & Associates. Since introduced, NeXpose has been sold to corporate enterprises, Global 2000 companies, and government entities, and serves the full range of vertical markets across the U.S. and abroad. Rapid7 is headquartered in Boston, MA, with offices in California and the United Kingdom. For more information on the company and its product, NeXpose, visit <http://www.rapid7.com>.