

COT Security Alert - Vulnerability in Multiple Adobe Products

A vulnerability has been discovered in the Adobe Acrobat, Adobe Reader and Adobe Flash Player applications.

This involves:

- Flash Player 10.0.45.2, 9.0.262, and earlier 10.0.x and 9.0.x versions
- Adobe Reader and Acrobat 9.3.2 and earlier 9.x versions

Adobe Reader 9.x and Adobe Acrobat 9.x products are vulnerable via the 'authplay.dll' which allows those products to view Flash content within PDF files. Adobe Reader 8.x and Adobe Acrobat 8.x are not vulnerable.

Exploitation can occur if a user visits a malicious webpage or opens a malicious file, including an email attachment. Successful attackers could execute code on affected systems allowing them to gain the same privileges as the logged on user. Depending on these privileges, attackers could install programs; view, change or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

This vulnerability is actively being exploited over the Internet and there is no Adobe patch available at this time. While antivirus updates may address known exploits as they arise, new exploits may be created and released against the vulnerability until a patch from the software vendor is available.

The following actions may be taken to reduce the effectiveness of the vulnerability:

- Install the appropriate Adobe patch as soon as it becomes available after appropriate testing.
- Ensure that all antivirus software is up to date with the latest signatures.
- If you believe you have been affected by attacks exploiting this vulnerability, please report the incident to CommonwealthServiceDesk@ky.gov.
- Run software as a non-privileged user (one without administrative privileges) where possible to diminish the effects of a successful attack.
- Caution users never to open attachments in unexpected emails. In this case, particular caution of any .pdf or .swf files is advised.
- Caution users not to open .pdf documents on web pages except as necessary on trusted sites.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
<http://technology.ky.gov/security/>