

---

**From:** Weber, Lon on behalf of CNRHelpDesk  
**Sent:** Thursday, January 14, 2010 9:22 AM  
**To:** CNRHelpDesk  
**Subject:** RE: Really Bad Adobe 0-Day Exploit

**Importance:** High

Hello CNR,

Adobe has finally patched the nasty security hole in both their Adobe Acrobat and Reader applications. Note that this vulnerability and patch is for both the Microsoft Windows and Apple OS X operating systems. You should follow the following steps to update your Adobe Acrobat and Reader programs ASAP on both OS's. You can refer to my original email (below) for help with determining which Adobe products you have installed. Remember that this is only for Adobe Acrobat 7.x, 8.x, 9.x and Adobe Reader 7.x, 8.x, 9.x. As always please feel free to contact Chad at [CNRHelpDesk@exchange.vt.edu](mailto:CNRHelpDesk@exchange.vt.edu) (1-9599) for questions or assistance. Thanks. Lon.

Steps to patch the Adobe products:

1. Save any work as this update may require a restart.
2. Start up the affected product.
3. From the "Help" menu select "Check for Updates...".
4. Install any updates that it finds.
5. Repeat steps 2 through 4 until it says there aren't any more updates for each of the affected Adobe products.
6. Done.

FYI: Google along with around 20+ other major companies were compromised via this Adobe vulnerability!

=====

Lon A. Weber, Director of IT  
College of Natural Resources, Virginia Tech  
216C Cheatham Hall  
Blacksburg, VA 24061  
Phone: 540-231-3277 Fax: 540-231-7664

---

**From:** Weber, Lon **On Behalf Of** CNRHelpDesk  
**Sent:** Tuesday, December 15, 2009 10:39 AM  
**To:** CNRHelpDesk  
**Subject:** Really Bad Adobe 0-Day Exploit  
**Importance:** High

Hello CNR,

Adobe has just announced an "Extremely Critical" vulnerability in both their Acrobat and Reader product lines and it includes versions 7.x, 8.x, and 9.x. It is unclear at this time if this affects OS X as well so I suggest erring on the side of caution and doing this on Macs as well. This rating is as bad as it gets and to make it worse it is a 0-day exploit which means it is currently being used to take over users' computers. The bad news is that

there is not a patch available yet nor have they discussed when one will be available. **However, there is a relatively easy workaround that everyone SHOULD do ASAP for all the Adobe Acrobat/Reader products installed on all of your computers.** One easy way to see all the Adobe products you have installed in Windows is to look at the “Currently installed programs:” list in the “Add or Remove Programs” applet in the “Control Panel”. On the Mac you can use “Spotlight” to search for Adobe products or just look in your “Applications” folder. Also, remember to **NEVER** open unknown or unsolicited PDF attachments or click on PDF links on web pages that are not trusted or known. Thanks. Lon.

Steps for each Adobe Acrobat/Reader product installed on your computers: (Will not require a restart)

1. Launch the program.
2. Click on the “Edit” menu (“Adobe” menu on the Mac).
3. Select the “Preferences...” menu option.
4. Click on “JavaScript” in the “Categories” column on the left side of the window that appears.
5. Uncheck the “Enable Acrobat JavaScript” option near the top of the window.
6. Click on the “OK” button.
7. Quit the program.
8. Repeat for all Adobe Acrobat/Reader products that you have installed.
9. Done.

=====  
Lon A. Weber  
Director of IT, College of Natural Resources  
Virginia Tech  
540-231-3277 (Monday-Tuesday, Thursday-Friday)  
540-231-4962 (Wednesday)  
fax: 540-231-7664