

Forum:[Hack Forums](#)

Thread: [\[BHCPU\] Update your Adobe Programs NOW - Critical Updates released](#)

Aura - August 13, 2014, 5:13 am

Hey guys, Aura here with another [WARNING] thread.

Today, Adobe released many updates on its products : Adobe Flash Player, Adobe AIR, Adobe Flash Player and Adobe Acrobat to patch exploits and vulnerabilities that are considered "critical". These vulnerabilities are classified as real 0-days exploits that could allow an attacker to bypass the sandbox protection of Adobe products and elevated access under Windows to run native code and therefore, remotely control/excute code on the target machine.

The CVE-2014-0546 was reported by members of the Kaspersky Lab Global Research and Analysis Team, directors Costin Raiu and Vitaly Kamluk. They didn't disclose technical information on the exploit yet as they don't want to jump the fence too quick before the end of the investigation. They however confirm that this exploit was used in the wild in some recent exploits in some limited environment.

Adobe suggests you to update your Adobe Reader, Adobe Acrobat, Adobe Flash Player and Adobe AIR programs as soon as possible via their Automatic Updater or by download the latest version of these programs from their website. Adobe is known to offer McAfee Security Scan Plus or another PUP on Adobe products download page when you download the installer, so please be sure to uncheck that promotional offer before clicking on the Download button..

Quote:Adobe Releases Critical Security Updates for Flash Player, Acrobat and Adobe Reader

Adobe has released security updates to fix seven vulnerabilities in its Flash and Air platforms and one in its Reader and Acrobat which, according to the company, is being exploited by attackers in wild "...in limited, isolated attacks targeting Adobe Reader users on Windows."

The vulnerabilities could allow an attacker to "take control of affected systems" marked critical by the company.

A new, out-of-band patch addresses a zero-day vulnerability (CVE-2014-0546) in Adobe Reader and Acrobat that offers an attacker the possibility to bypass sandbox protection and has been leveraged in "limited, isolated attacks" against Windows users.

"These updates resolve a sandbox bypass vulnerability that could be exploited to run native code with escalated privileges on Windows," Adobe warned.

The lone vulnerability in Adobe Acrobat and Reader was reported by Kaspersky Lab Global Research and Analysis Team director Costin Raiu and Vitaly Kamluk.

However, details of the vulnerability were not disclosed, but Raiu said in a blog post that exploits have been observed in a rare number of targeted attacks, and that it's still important for everyone to patch as soon as possible.

“At the moment, we are not providing any details on these attacks as the investigation is still ongoing,” Raiu said. “Although these attacks are very rare, just to stay on the safe side we recommend everyone to get the update from the Adobe site as soon as possible.”

The Apple OS X versions of Acrobat and Reader are not vulnerable. Only Reader and Acrobat versions 11.0.07 and earlier for Windows are affected, according to the company.

The other security update patches seven vulnerabilities in Flash Player, most of which are rated critical by the company, but none of the Flash vulnerabilities are being exploited in the wild, Adobe said.

Five of the updates resolved memory leakage vulnerabilities that can be used to bypass memory address randomization. Rest two patches address a security bypass vulnerability and a use-after-free flaw that could allow an attacker to remotely execute code on the affected system.

The affected versions are as follow: Adobe Flash Player 14.0.0.145 and earlier versions for Windows and Macintosh

Adobe Flash Player 11.2.202.394 and earlier versions for Linux

Adobe AIR 14.0.0.110 and earlier versions for Windows and Macintosh

Adobe AIR 14.0.0.137 SDK and earlier versions

Adobe AIR 14.0.0.137 SDK & Compiler and earlier versions

Adobe AIR 14.0.0.137 and earlier versions for Android

The company urged its users to apply the updates within three days on Windows, Mac, and Linux platforms. Users may update Acrobat and Reader with the Help > Check for Updates menu option. Flash Player users may download the latest version from Adobe. Users of Internet Explorer and Google Chrome on Windows 8 and above will receive browser updates from those companies with fixed versions of their integrated Flash Player.

Microsoft has also rolled out nine security updates to address at least 37 security holes in Windows and related software, including Internet Explorer, Windows Media Center, One Note, SQL Server, and SharePoint.

The company has also made some important changes this month. Microsoft announced that it will soon begin blocking out-of-date ActiveX controls for Internet Explorer users, and will support only the latest versions of the .NET Framework and IE for each supported operating system.

Adobe products are part of the most exploited products by malware, hackers, etc. in order to infect and take over system running these products. It's is vital to maintain these products up to date if you use it, or disable/uninstall them if you don't use it. It's one of the basics of Computer Protection and everyone should know that.

Please update your Adobe Reader, Acrobat, Flash Player and AIR as soon as possible to be less vulnerable and to patch your programs against theses exploits.

Thank you.

Reticulum - August 13, 2014, 5:25 am

Thank you Aura, I guess it's a good thing I only have Air and Reader, updating now.

Edit: Why hasn't someone made an AV/White Hat tool that auto updates everything, like Adobe, Java, etc? It seems like it'd be rather helpful for forgetful people or ones who just aren't informed.

Aura - August 13, 2014, 5:28 am

(Aug 13, 2014 05:25 AM)Ridge™ Wrote: [\[CITE\]](#) Thank you Aura, I guess it's a good thing I only have Air and Reader, updating now.

Edit: Why hasn't someone made an AV/White Hat tool that auto updates everything, like Adobe, Java, etc? It seems like it'd be rather helpful for forgetful people or ones who just aren't informed. There is. Look up Hippo Update Checker and SecuniaPSI (that I use).

Also, all these programs have auto-updaters that if enabled and set correctly, will auto-update the programs when new updates are released.

Reticulum - August 13, 2014, 5:32 am

So this might be a stupid question but get.adobe.com is the legit domain correct? If so why does the Reader file look so "unprofessional" name wise, and the download location is strange as well compared to Air.

Aura - August 13, 2014, 5:38 am

(Aug 13, 2014 05:32 AM)Ridge™ Wrote: [\[CITE\]](#) So this might be a stupid question but get.adobe.com is the legit domain correct? If so why does the Reader file look so "unprofessional" name wise, and the download location is strange as well compared to Air.

Yes it's the legitimate download website for these products.

And I wouldn't know, ask Adobe about that. I don't know what kind of nomenclature they use for their file name and download location ?

/Ninja - August 15, 2014, 10:47 am

Thanks for the heads up Aura. I got prompted for a flash update the other day but i wasn't sure if i could trust it. I don't know why i just didn't feel right.

Thanks!

Aura - August 15, 2014, 10:55 am

(Aug 15, 2014 10:47 AM)/Ninja Wrote: [\[CITE\]](#) Thanks for the heads up Aura. I got prompted for a flash update the other day but i wasn't sure if i could trust it. I don't know why i just didn't feel right.

Thanks!

It's hard now a day to trust Adobe products updates pop-up as they are everywhere. But if it's launched from your icon tray, it's their auto-updater so it's good.

/Ninja - August 15, 2014, 9:48 pm

(Aug 15, 2014 10:55 AM)Aur? Wrote: [\[CITE\]](#) It's hard now a day to trust Adobe products updates pop-up as they are everywhere. But if it's launched from your icon tray, it's their auto-updater so it's good.

Yeah did a double check and made sure. All updated and safe :)

Gary - August 16, 2014, 8:09 pm

(Aug 13, 2014 05:32 AM)Ridge™ Wrote: [\[CITE\]](#) So this might be a stupid question but get.adobe.com is the legit domain correct? If so why does the Reader file look so "unprofessional" name wise, and the download location is strange as well compared to Air.

Its a legit domain as it redirects to <http://www.adobe.com/ca/> at least for me.