

Forum:[Hack Forums](#)

Thread: [Adobe Flash Player Update Patches 11 Critical Vulnerabilities](#)

NoScript - March 13, 2015, 7:20 pm

The Hacker News Wrote: After the latest Microsoft Patch Tuesday updates that came with important patches for Stuxnet and FREAK encryption-downgrade attack, now its time to update your Adobe Flash Player.

Adobe has rolled-out an update for its popular Flash Player software that patches a set of 11 critical security vulnerabilities in its program, most of which potentially allow hackers to remotely execute arbitrary code on vulnerable systems.

AFFECTED SOFTWARE

All versions prior to the latest version 17.0.0.134 of the Flash Player are affected on Windows and Mac OS X machines. Therefore, Adobe Flash Player installed with Google Chrome, as well as Internet Explorer 10 and 11 on Windows 8 and Windows 8.1, should automatically update to the newest version 17.0.0.134.

In addition, Adobe Flash Player 11.2.202.442 for Linux and Flash Player Extended Support Release 13.0.0.269 for Windows and Mac OS X are also affected by the vulnerabilities.

So, users of Flash Player on Linux should update to version 11.2.202.451 and Flash Player Extended Support Release on Windows and Mac are recommended to update to version 13.0.0.277.

REMOTE CODE EXECUTION

Total 9 Remote Code Execution vulnerabilities patches are included in the latest Adobe Flash Player update. An attacker could serve a specially crafted Flash file to trigger the vulnerabilities, which would lead to the execution of attacker's code in order to take control of a target system.

Most of the vulnerabilities in Adobe Flash Player have been reported by security researchers from Google's Project Zero team. Other security companies that disclosed the vulnerabilities are Hewlett-Packard, NCC Group, Intel and McAfee.

LIST OF VULNERABILITIES

The list of all the patched vulnerabilities along with their impacts is given below: CVE-2014-0332 — Remote code execution via memory corruption vulnerability.

CVE-2015-0333 — Remote code execution via memory corruption vulnerability.

CVE-2015-0334 — Remote code execution from type confusion vulnerability.

CVE-2015-0335 — Remote code execution via memory corruption vulnerability.

CVE-2015-0336 — Remote code execution from type confusion vulnerability.

CVE-2015-0337 — A 'cross domain policy bypass' flaw.

CVE-2015-0338 — Remote code execution from integer overflow vulnerability.

CVE-2015-0339 — Remote code execution via memory corruption vulnerability.

CVE-2015-0340 — A 'File upload restriction bypass' flaw.

CVE-2015-0341 — Remote code execution from a 'use-after-free' vulnerability.

CVE-2015-0342 — Remote code execution from a 'use-after-free' vulnerability.

According to Adobe, none of the vulnerabilities are being publicly exploited in the wild thus far. However, we all know that immediately after the the release of updated versions, hackers starts exploiting these critical flaws in order to catch out people who haven't updated their machines.

Therefore users and administrators running Adobe Flash Player on Windows, Mac OS X and Linux are advised to update their software to the most recent version of the software in an attempt to protect their systems from cyber attacks.

Source: <http://thehackernews.com/2015/03/adobe-flash-player-update.html>

It is highly recommended that you either uninstall or update your adobe flash player to guard yourself from these vulnerabilities in unpatched versions.

Aceman - March 14, 2015, 8:12 am

Adobe has way too many vulnerabilities too frequently.

NoScript - March 14, 2015, 8:47 am

(Mar 14, 2015 08:12 AM)Aceman Wrote: [\[CITE\]](#) Adobe has way too many vulnerabilities too frequently.

Yes, but at least they are finally patching them ?

He B TeMy - March 14, 2015, 3:44 pm

(Mar 14, 2015 08:47 AM)Truffle Wrote: [\[CITE\]](#) Yes, but at least they are finally patching them ?
What he was saying is, next week there's another 10.

I'm seriously baffled of how many vulnerabilities have been found in Adobe Flash, for real, it's been here for over a decade, used by millions everyday, still vulnerable as fuck.

I know a system can't be ever bulletproof but...