Are the Adobe Flash Vulnerabilities Leaving You Feeling Scared?

Based on an analysis in 2015 of over 100 exploit kits (EKs) and known vulnerabilities, Adobe Flash was the unfortunate winner of the most frequently exploited product. With 2017 around the corner, companies are joking that maybe it's time to give Flash the old heave ho' to retirement. While Adobe has worked tirelessly to make Flash more secure, improving the decades old application is proving to be a grave task.

In reality, security shouldn't be joked about. While regular monthly and emergency zero-day flaw patches are released, Adobe Flash vulnerabilities continue to threaten secure operating environments.

Adobe Flash Vulnerabilities

This year, six of the top 10 vulnerabilities incorporated by exploit kits affected Adobe Flash Player. The most common vulnerability found was CVE-2016-0189 – 700 web sources linked it to Magnitude, RIG, Neutrino, and Sundown exploit kits.

Other Adobe Flash vulnerabilities include:
CVE-2016-1o1o and CVE-2015-8446 – linked to Angler
CVE-2016-1019, CVE-2016-4117, and CVE-2015-8651 – linked to at least three exploit kits
CVE-2015-7645 – linked to seven different packages

The last vulnerability listed impacts Windows, Mac, and Linux operating systems, allowing threat actors to take control of the affected system. It was also the first zero-day exploit uncovered after Adobe released new security mitigations. With the phase out of unsupported vulnerabilities, rapid adoption ensued, including the Russian government-backed espionage group, Pawn Storm (APT28, Fancy Bear).

Most recently, Adobe has patched 31 vulnerabilities across nine different product lines, including a zero-day vulnerability in Flash Player (CVE-2016-7892). The vulnerability is designed to target users of Internet Explorer on Windows machines. While little detail is currently known, it seems that the focus of attacks is on the 32-bit version of IE.

Browsers Take a Stand Against Flash

Internet Explorer is about to be the only widely used browser to run Flash-powered animations and video out of the box. Microsoft is the newest member on the anti-Flash bandwagon to commit to disabling Adobe Flash. By default, Windows 10's Edge browser will come without Flash to provide dynamic content.

So what's the option besides Flash? HTML5. And it is on the rise as a secure and fast alternative to playing video and animation. Google Chrome, Mozilla Firefox, and Apple Safari browsers are all moving to the new technology. Users will only encounter Flash if they actively click and trigger it. For security experts this is great news. Hopefully as Flash fades into the background, there will be a seamless transition to HTML5. This is especially true when users prefer the faster and more reliable way of viewing.

Prepare for the Death of Adobe Flash

It's only a matter of time until the Adobe Flash vulnerabilities catch up to the multimedia software platform. Security holes, crashes, and poor performance over decades don't bode well for a product's success.

While we haven't attended the funeral for Flash just yet, web developers should keep in mind the transition to HTML5 while working. It's going to be imperative to move away from a product that has new vulnerabilities discovered all the time. Especially when the majority allow for remote code execution by hackers.

If you've had enough of malware attacks because of Adobe Flash vulnerabilities, it's probably time to use endpoint protection. Download our free Next Generation Endpoint Protection Buyer's Guide to learn more.