NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

CONTINUED USE OF ADOBE FLASH INVITES COMPROMISE

DISCUSSION

On July 25, 2017, Adobe® Inc. announced they will stop updating and distributing Flash®[1] by the end of 2020.[2] Adobe is encouraging content creators to migrate Flash® content to open-source, standards-based technologies, such as HTML5, WebGL and WebAssembly.[2]

Since the release of Flash®, Adobe has patched over 840 code-execution vulnerabilities in it.[3] When Adobe ends support in 2020, no new patches should be expected for newly reported vulnerabilities. Systems that continue to use Flash® are at an increased risk of compromise. Flash® vulnerabilities discovered after 2020 will become permanent attack vectors into systems running the software. Adversaries can easily exploit outdated software, often using nothing more than public information. Any publicly unknown Flash® vulnerabilities prior to 2020 will also continue to be successfully leveraged by attackers. With 2020 fast approaching, failing to remove Flash® places systems at increased risk of compromise.

Industry has widely agreed with Adobe's decision to end support of Flash® with Mozilla Firefox™[4], Google Chrome™[5], Apple Safari®[6], and Microsoft Edge®[7] removing Flash® support by the end of 2020. Updating browsers as soon as updates are available, and removing end-of-life software before the end-of-life deadline, are both vital to protecting systems.

MITIGATION ACTIONS

On web servers, system administrators should stop hosting Flash® applications. Continuing to host Flash® applications will force the use of old, unpatched browsers that are vulnerable to exploitation. Web developers should convert Flash® applications to a newer, more secure technology. Replacing Flash® with standards-based technologies, such as HTML5, WebGL, and WebAssembly, is critical to lowering risk of exploitation.

On end-user systems, administrators or users should remove Flash® from browsers. Use a fully automated process for updating browsers and always update browsers to the latest version. Enabling the automatic update feature in modern browsers is the only reliable way for internet-connected systems to keep the browser updated.

For additional information on browser security, see Steps to Secure Web Browsing which can be found at:
https://nsa.gov/what-we-do/cybersecurity/advisories-technical-guidance

Adobe guidance for converting Flash® to HTML5 can be found at:
https://helpx.adobe.com/animate/how-to/convert-flash-ads-to-html5.html
https://helpx.adobe.com/animate/how-to/convert-flash-to-html5.html

---

[1] Adobe and Flash are either registered trademarks or trademarks of Adobe Inc. in the United States and/or other countries. Mozilla and Firefox are trademarks of the Mozilla Foundation in the U.S. and other countries. Google Chrome is a trademark of Google, LLC. Apple and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. Microsoft Edge is a registered trademark of Microsoft Corporation in the United States and other countries.

[2] Flash and the Future of Interactive Content. https://theblog.adobe.com/adobe-flash-update

[3] Adobe Flash Player Vulnerability Statistics. https://www.cvedetails.com/product/6761/Adobe-Flash-Player.html?vendor_id=53

[4] Firefox Roadmap for Flash End-of-Life. https://blog.mozilla.org/futurereleases/2017/07/25/firefox-roadmap-flash-end-life

[5] Saying Goodbye to Flash in Chrome. https://www.blog.google/products/chrome/saying-goodbye-flash-chrome

[6] Adobe Announces Flash Distribution and Updates to End. https://webkit.org/blog/7839/adobe-announces-flash-distribution-and-updates-to-end

[7] The End of an Era – Next Steps for Adobe Flash. https://blogs.windows.com/msedgedev/2017/07/25/flash-on-windows-timeline

DISCLAIMER OF WARRANTIES AND ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or endorsement purposes.

NOTICE

The information contained in this document was developed in the course of NSA's cybersecurity missions including its responsibilities to identify and disseminate threats to national security systems and Department of Defense information technologies, develop and issue security implementation specifications for cybersecurity-enabled products, and to assist Executive departments and agencies with operational security programs. The information may be shared broadly to reach all appropriate stakeholders.

CONTACT

Cybersecurity Requirements Center
410-854-4200
Cybersecurity_Requests@nsa.gov