computer emergency response team CERT-EU
for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2018-005

Critical Vulnerability in Adobe Flash Player

February 07, 2018 — v1.1

History:

- *06/02/2018 — v1.0: Initial publication*
- *07/02/2018 — v1.1: Patch released*

Summary

On January 31, 2018, KrCERT/CC released a security alert regarding a vulnerability in Adobe Flash Player [1]. Regarding this issue, Adobe Systems has also released a security advisory about the vulnerability (CVE-2018-4878). According to Adobe, the vulnerability is being exploited in the wild. As of February 6th, 2017 a patch from Adobe is available [5].

Technical Details

The vulnerability received the following CVE: CVE-2018-4878.

The technical details concerning this vulnerability have not been disclosed yet, but the information published so far has shown that remote attackers leveraging this vulnerability may be able to execute arbitrary code.

According Talos Group [2], the exploit is being distributed through a Microsoft Excel document that has a malicious Flash object embedded into it. Once the SWF object is triggered, it installs ROKRAT, a remote administration tool. So far the incidents known related to this vulnerability seem to be geographically centered on Korea.

Products Affected

According to Adobe this are the affected versions [1]:

- Adobe Flash Player Desktop Runtime 28.0.0.137 and earlier versions Windows, Macintosh
- Adobe Flash Player for Google Chrome 28.0.0.137 and earlier versions Windows, Macintosh, Linux and Chrome OS
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 28.0.0.137 and earlier versions Windows 10 and 8.1
- Adobe Flash Player Desktop Runtime 28.0.0.137 and earlier versions Linux

To verify the version of Adobe Flash Player installed on your system, access the About Flash Player page, or right-click on content running in Flash Player and select **About Adobe (or Macromedia) Flash Player** from the menu. If you use multiple browsers, perform the check for each browser you have installed on your system.

Recommendations

Adobe has released a patch for this vulnerability, review its security bulletin [5] to choose the proper patch.

Also, since Adobe Flash is deprecated, you should consider migrating any still used Adobe Flash to HMTL5.

Mitigations

If for whatever reason the patch cannot be installed, the following workarounds may be considered:

- Disable Adobe Flash on your browser or enable click-to-play in order to avoid running undesired content.
- According Adobe, on Internet Explorer with Adobe Flash Player version 27 or later and on Windows 7 or later, it is possible to display a prompt screen when SWF content is played. Review the Administration Guide [3].
- Since the detected exploits were embedded on Microsoft Office documents, consider setting up Protected Views on them [4].

References

[1] https://helpx.adobe.com/security/products/flash-player/apsa18-01.html

[2] http://blog.talosintelligence.com/2018/02/group-123-goes-wild.html?

[3] https://www.adobe.com/content/dam/acom/en/devnet/flashplayer/articles/flash_player_admin_guide/pdf/flash_player_27_0_admin_guide.pdf

[4] https://support.office.com/en-us/article/what-is-protected-view-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653#bm5

[5] https://helpx.adobe.com/security/products/flash-player/apsb18-03.html