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

### CERT-EU Security Advisory 2017-022

# Actively Exploited Critical Zero-Day Vulnerability in Adobe Flash

***October 17, 2017 — v1.0***

*History:*

- *17/10/2017 — v1.0: Initial publication*

## Summary

On 16th of October 2017, Adobe has released a security update for Adobe Flash Player for Windows, MacOS, Linux and Chrome OS. This update addresses a critical *type confusion* vulnerability that could lead to code execution (CVE-2017-11292) [1].

Adobe also alerted that this vulnerability is being actively exploited in targeted attacks. The exploit was identified on 10th of October by Kaspersky's researchers [2].

## Technical Details

The vulnerability is a memory corruption vulnerability that exists in the following class:

```
com.adobe.tvsdk.mediacore.BufferControlParameters
```

Once the exploit is successful, the attacker gains arbitrary read/write operations within memory, thus leading to code execution in the context of the user.

Kaspersky's researchers spotted the malicious code delivered via an MS Office document, embedded in an ActiveX object [2].

## Products Affected

- Adobe Flash Player Desktop Runtime 27.0.0.159 on Windows, MacOS, and Linux
- Adobe Flash Player for Google Chrome 27.0.0.159 on Windows, MacOS, Linux, and Chrome OS
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 27.0.0.130 on Windows 10 and Windows 8.1

## Recommendations

Apply security update issued by Adobe [1]:

- Adobe Flash Player Desktop Runtime 27.0.0.170 on Windows, MacOS, and Linux
- Adobe Flash Player for Google Chrome 27.0.0.170 on Windows, MacOS, Linux, and Chrome OS
- Adobe Flash Player for Microsoft Edge and Internet Explorer 11 27.0.0.170 on Windows 10 and Windows 8.1

Concerning Flash player for Google Chrome, it will be automatically updated to the latest Google Chrome version.

## References

[1] Adobe advisory https://helpx.adobe.com/security/products/flash-player/apsb17-32.html

[2] Kaspersky Blog post about BlackOasis APT https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/