



Q-CERT Advisory

Critical Adobe Flash Player Vulnerability CVE-2017-11292

Release Date: Oct, 18 2017

Introduction A critical vulnerability (CVE-2017-11292) has been identified in Adobe Flash Player / Desktop Runtime version (27.0.0.159) and earlier versions for Windows, Macintosh and Linux. Adobe is aware of a report that an exploit for this vulnerability is being used in limited, targeted attacks. This vulnerability is found to be used by the BlackOasis (a threat actor identified by Kaspersky Labs) targeted attacks campaign. Adobe has released security patch for fixing (CVE-2017-11292) on October 16, 2017.

Impact An attacker succeeding to exploit this vulnerability can:

- gain arbitrary read / write operations within memory.
- execute a second stage shellcode leading to a arbitrary code execution.

Affected Systems

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

Solution Adobe has released a security patch to fix CVE-2017-11292 and other in the following link: <https://helpx.adobe.com/security/products/flash-player/apsb17-32.html>

Reporting Q-CERT Team will be available for Emergency Response on 24x7 basis through the following contacts:

Q-CERT Hotline : +974 - 44933408 / +974 - 44995399 Q-CERT

E-Mail: incidents@qcert.org

References For more details find the following references:

- <https://helpx.adobe.com/security/products/flash-player/apsb17-32.html>
- <https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/>

