INCIDENTS RESEARCH

CVE-2016-4171 – Adobe Flash Zero-day used in targeted attacks

By Costin Raiu on June 14, 2016. 6:38 pm

Earlier today, Adobe published the security advisory APSA16-03, which describes a critical vulnerability in Adobe Flash Player version 21.0.0.242 and earlier versions for Windows, Macintosh, Linux, and Chrome OS:

> Adobe is aware of a report that an exploit for CVE-2016-4171 exists in the wild, and is being used in limited, targeted attacks. Adobe will address this vulnerability in our monthly security update, which will be available as early as June 16. For the latest information, users may monitor the Adobe Product Security Incident Response Team blog.

Severity ratings

Adobe categorizes this as a critical vulnerability.

Acknowledgments

Adobe would like to thank Anton Ivanov and Costin Raiu of Kaspersky for reporting CVE-2016-4171 and for working with Adobe to help protect our customers.

A few of months ago, we deployed a new set of technologies into our products designed to identify and block zero day attacks. These technologies already proved its effectiveness earlier this year, when they caught an Adobe Flash zero day exploit, CVE-2016-1010. Earlier this month, we caught another zero-day Adobe Flash Player exploit deployed in targeted attacks.

We believe these attacks are launched by an APT Group we call "ScarCruft".

ScarCruft is a relatively new APT group; victims have been observed in several countries, including Russia, Nepal, South Korea, China, India, Kuwait and Romania. The group has several ongoing operations utilizing multiple exploits — two for Adobe Flash and one for Microsoft Internet Explorer.

Currently, the group is engaged in two major operations: **Operation Daybreak** and **Operation Erebus**. The first of them, Operation Daybreak, appears to have been launched by ScarCruft in March 2016 and employs a previously unknown (0-day) Adobe Flash Player exploit, focusing on high profile victims. The other one, "Operation Erebus" employs an older exploit, for CVE-2016-4117 and leverages watering holes. It is also possible that the group deployed another zero day exploit, CVE-2016-0147, which was patched in April.

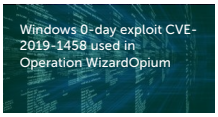
We will publish more details about the attack once Adobe patches the vulnerability, which should be on June 16. Until then, we confirm that Microsoft EMET is effective at mitigating the attacks. Additionally, our products detect and block the exploit, as well as the malware used by the ScarCruft APT threat actor.

** More information about the ScarCruft APT and Operation Daybreak is available to customers of Kaspersky Intelligence Services. Contact: intelreports@kaspersky.com*

ADOBE FLASH APT VULNERABILITIES ZERO-DAY VULNERABILITIES

Share post on:

Related Posts



LEAVE A REPLY

Your email address will not be published. Required fields are marked *

Enter your comment here

Name *

Email *

Save my name, email, and website in this browser for the next time I comment.

SUBMIT

IN THE SAME CATEGORY


Assessing the impact of protection from web miners


An advertising dropper in Google Play


Agent 1433: remote attack on Microsoft SQL Server


How to steal a million (of your data)


On the IoT road: perks, benefits and security of moving smartly