Tonga National Computer Emergency Response Team

New Zero-day Vulnerability in Adobe Flash Player

Dear Constituents,

Flash Player zero-day exploit was spotted by researchers inside malicious Microsoft Office documents, which were submitted to online multi-engine malware scanning service VirusTotal from a Ukrainian IP address.The vulnerability, tracked as **CVE-2018-15982**, is a use-after-free flaw resides in Flash Player that, if exploited successfully, allows an attacker to execute arbitrary code on the targeted computer and eventually gain full control over the system.

How it works

1. The maliciously crafted Microsoft Office documents contain an embedded Flash Active X control in its header that renders when the targeted user opens it, causing exploitation of the reported Flash player vulnerability.

2. According to cybersecurity researchers, neither the Microsoft Office file (22.docx) nor the Flash exploit (inside it) itself contain the final payload to take control over the system.

3. Instead, the final payload is hiding inside an image file, which is itself an archive file, that has been packed along with the Microsoft Office file inside a parent WinRAR archive which is then distributed through spear-phishing emails

4. Upon opening the document, the Flash exploit executes a command on the system to unarchive the image file and run the final payload (i.e., backup.exe) which has been protected with VMProtect and programmed to install a backdoor that is capable of:
    - monitoring user activities (keyboard or moves the mouse)
    - collecting system information and sending it to a remote command-and-control (C&C) server,
    - executing shellcode,
    - loading PE in memory,
    - downloading files
    - execute code, and
    - performing self-destruction.

What to do

1) Update your systems with the latest patches to prevent abuse of vulnerabilities.

2) Disable or uninstall Adobe Flash Player from their systems until Adobe issues a patch

Reference:

- https://blog.malwarebytes.com/malwarebytes-news/2018/12/new-flash-player-zero-day-used-russian-facility/
- https://helpx.adobe.com/security/products/flash-player/apsb18-42.html

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
OG Sanft Building Level 2
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.to
web: www.cert.to