Microsoft Patch Tuesday updates for May 2017 fix Zero Days exploited by Russian APT groups

May 10, 2017 By Pierluigi Paganini

Microsoft Patch Tuesday for May 2017 address tens security vulnerabilities, including a number of zero-day flaws exploited by Russian APT groups.

Microsoft Patch Tuesday updates for May 2017 fix more than 50 security flaws, including a number of zero-day vulnerabilities exploited by Russian APT groups.

Microsoft released security updates for Windows, Internet Explorer, Edge, Office, the .NET framework, and Flash Player on Tuesday.

Security experts at Microsoft worked with peers at ESET and FireEye to address the vulnerabilities affecting Encapsulated PostScript (EPS) filter in Office.

Researchers at FireEye investigated some attacks attributed to the Russian APT groups and also an unknown financially-motivated threat actor.

"At the end of March 2017, we detected another malicious document leveraging an unknown vulnerability in EPS and a recently patched vulnerability in Windows Graphics Device Interface (GDI) to drop malware. Following the April 2017 Patch Tuesday, in which Microsoft disabled EPS, FireEye detected a second unknown vulnerability in EPS." reads the analysis shared by FireEye.

"FireEye believes that two actors – Turla and an unknown financially motivated actor – were using the first EPS zero-day (CVE-2017-0261), and APT28 was using the second EPS zero-day (CVE-2017-0262) along with a new Escalation of Privilege (EOP) zero-day (CVE-2017-0263). Turla and APT28 are Russian cyber espionage groups that have used these zero-days against European diplomatic and military entities. The unidentified financial group targeted regional and global banks with offices in the Middle East."

The Turla group (aka Waterbug, KRYPTON, and Venomous Bear) has been exploiting an Office remote code execution (RCE) vulnerability (CVE-2017-0261) to spread the SHIRIME custom JavaScript malware.

A second group of financially motivated threat actors has been exploiting the same vulnerability to deliver a new variant of the NETWIRE malware.

The experts observed that The Turla APT also leveraged CVE-2017-0001 for privilege escalation, while the cyber crime gang the CVE-216-7255 for privilege escalation.

The experts from the two firms confirmed that the notorious APT28 group exploited a number of zero-day vulnerabilities in targeted attacks, including the CVE-2017-0262 Office RCE vulnerabilities and a Windows privilege escalation tracked as CVE-2017-0263.

The hackers leveraged the above exploits to deliver the GAMEFISH malware (Seduploader).

Microsoft announced that the security updates released this month have fixed vulnerabilities in Office (CVE-2017-0261 and CVE-2017-0262) exploited the Russian APT groups.

The list of flaws fixed by Microsoft on Tuesday includes also a memory corruption issue in Internet Explorer tracked as CVE-2017-0222, this memory corruption zero-day can be exploited by a remote attacker for code execution.

Pierluigi Paganini

(Security Affairs – *Russian APT groups*, APT28)

Share this...

APT28 | cyber espionage | Cybercrime | Hacking | Russian APT groups | Turla | zero-Day

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS ARTICLE
Adobe fixes critical and important flaws in Flash Player and Experience Manager

NEXT ARTICLE
The Rakos botnet - Exploring a P2P Transient Botnet From Discovery to Enumeration

YOU MIGHT ALSO LIKE

Pwn2Own 2020 Day1 -researchers earned $180K for hacking Windows, Ubuntu, and macOS

March 19, 2020 By Pierluigi Paganini

Cisco addresses multiple issues in its SD-WAN product

March 18, 2020 By Pierluigi Paganini

YOROI

Yoroi Blog