October 8 – October 14, 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Pentagon has admitted a breach where an attacker appear to have compromised a third-party contractor and used the vendor's access to the Pentagon network to steal travel data for Department of Defense personnel. This may have revealed personal and credit card information of at least 30,000 employees.

- Google has announced that it plans to shut down its social media network Google+, after the company suffered a massive data breach that exposed the private data of hundreds of thousands of Google Plus users to third-party developers. This breach has potentially affected up to 500,000 accounts.

- Financially motivated attackers have been exploiting the Drupal vulnerabilities, including Drupalgeddon2 and Drupalgeddon3, to install a backdoor on the infected systems and take full control of the hosted platforms.

  Check Point IPS blade provides protection against this threat (Drupal Core Remote Code Execution (CVE-2018-7600); Drupal Core Remote Code Execution (CVE-2018-7602))

- FitMetrix fitness software company has exposed millions of records of customer data online, publically available and unprotected. The exposed records include name, gender, email address, birth date, home and work phone, height, weight and much more.

- A new cyber espionage group has been revealed, tracked as “Gallmaker”. The group has targeted entities in the government, military and defense sectors in Eastern Europe and the Middle East since at least 2017, mainly using fileless attacks and publicly available hack tools.

- A new campaign lures victims to download a fake Adobe Flash update containing a code to download and execute an XMRig Cryptominer on Windows systems.

©2018 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

VULNERABILITIES AND PATCHES

- Microsoft has released its monthly Patch Tuesday update for October 2018, fixing a total of 49 security vulnerabilities in its products. Out of 49 flaws patched this month, 12 are rated as critical. In this batch, the company released a patch to a zero-day vulnerability in Win32k currently actively exploited by a Middle-East based APT dubbed FruityArmor. Another patch was issued for a zero-day vulnerability in JET, which third-party researchers have warned is incomplete, and released a micro-patch to fix it.

  Check Point IPS blade provides protection against this threat (Microsoft Win32k Elevation of Privilege (CVE-2018-8453))

- Adobe has released its monthly security update addressing 11 vulnerabilities in Adobe Digital Editions, Framemaker, and Technical Communications Suite, 4 of which are rated critical.

  Check Point IPS blade provides protection against these threats (Adobe Acrobat and Reader Out-of-bounds write (APSB18-30: CVE-2018-15955); Adobe Acrobat and Reader Out-of-bounds write (APSB18-30: CVE-2018-15954); and others)

- Juniper Networks has patched dozens of serious security vulnerabilities. The most severe flaw could be exploited by an attacker to crash the Junos kernel by sending specially crafted MPLS packets.

- Google Project Zero security researcher has found a critical vulnerability in WhatsApp messenger that may allow threat actors to remotely take full control of one's WhatsApp account by using the video call over the messaging app.

THREAT INTELLIGENCE REPORTS

- A security researcher has released proof-of-concept code to a remote code execution attack on an old directory traversal vulnerability. The new hacking technique was used against vulnerable MikroTik routers, allowing attackers to remotely execute code on affected devices and gain a root shell.

- A new malware for Android devices has been spotted in the wild dubbed "GPlayed", with capabilities of both banking Trojan and sophisticated cyber-espionage malware. GPlayed is also able to adapt after its deployment, allowing its operators to remotely load plugins, inject scripts and even compile and execute new .NET code on the device.

  Check Point SandBlast Mobile customers are protected from this threat

- Following the big "China-Hack" claiming china has added a microchip to motherboards that can be used for remote code execution, a supply chain security 101 view was published pinpointing the difficulties and challenges when facing compromised hardware scenarios.

For comments, please contact: TI-bulletin@checkpoint.com