June 15, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Intel CPU vulnerable to 'SGAxe' and 'CrossTalk' Side-channel Attack
- SMBleed: New critical vulnerability affects Windows SMB Protocol
- Windows 10 privacy bug lets users change admin option
- Messenger bug could have helped Malware gain persistence
- Black Lives Matter Emails used to deliver TrickBot Malware
- Two code execution vulnerabilities in Microsoft Excel

Introduction to InfoSec Weekly

InfoSec Weekly is a compilation of security related news feed that aims to update the readers about cyber security, cyber threats, malware attacks, new technologies and cyber security awareness every week. We primarily cover events and news related to offensive side of the Information Security such as hacking, password and sensitive information leakage, new vulnerabilities and important CVE's that can impact an individual or an organization. We also aim to provide defensive tactics to overcome known vulnerabilities that can protect organizations and individuals from any attacks.

Our main aim is to spread awareness regarding various cyber related threats.

About Us

We are a team of security enthusiasts with an aim to provide various Information Security Services to organizations. Our company aims to provide professional grade cyber security solutions for all your Information Technology infrastructures. Our team has been demonstrating penetration testing skills using methodologies such as OSSTMM, NIST and OWASP. We aim to help companies protect their valuable data from any internal or external threats. Our team members have been practicing their skills to detect and report vulnerabilities in a live environment. Organizations such as Google, Facebook, Twitter, Yahoo!, ebay, eset, bugcrowd, under armour, coinbase, CCM, etc have recognized our team members for reporting vulnerabilities and have helped these organizations from malicious users. Our team's professional work experience consists of various Government organizations, National and International based private organizations, INGOs, etc. Our Services ranges from VAPT, Incident Response, Information Security Training, Endpoint threat analysis, Cyber security consultant, etc.

1. Intel CPU vulnerable to 'SGAxe' and 'CrossTalk' Side-channel Attack

Description	
Cybersecurity researchers have identified two distinct attacks in Intel processors that could be exploited to gain sensitive information from CPU's trusted execution environment (TEE). SGAxe, one of the two flaws, is evolution of previously identified CachedOut attack which retrieved contents from CPU's L1 cache. CrossTalk allowed attacker-controlled code executing on one core to target SGX enclave running on another core to determine enclave's private key. Intel has released an updated firmware addressing the issue	
Source	https://thehackernews.com/2020/06/intel-sgaxe-crosstalk-attacks.html
Infected Technology	Intel processors
CVEs	CVE-2020-0549, CVE-2020-0543
Recommendation	Update the firmware released by Intel

2. SMBleed: New critical vulnerability affects Windows SMB Protocol

Description	
A new critical vulnerability, dubbed SMBleed, was uncovered by ZecOps that allowed remote attacker to leak kernel memory combined with wormable bug allows arbitrary code execution in the affected system. The vulnerability exists in Windows 10 version 1903 and 1909. The flaw is utilizing windows file sharing protocol, SMB, which runs over port 445 which was previously affected by SMBGhost. The previous vulnerability was fixed by Microsoft in March 2020 however the same decompression function has been affected by the new PoC. the decompression function in question ("Srv2DecompressData") handles specially crafted message requests (e.g., SMB2 WRITE) sent to a targeted SMBv3 server, allowing an attacker to read uninitialized kernel memory and make modifications to the compression function.	
Source	https://thehackernews.com/2020/06/SMBleed-smb-vulnerability.html?m=1
Infected Technology	Windows 10 version 1903, windows 10 version 1909, windows server version 1903, and windows server version 1909.
CVEs	CVE-2020-1206
Recommendation	Update the patch released by Windows Disable SMB unless used Block port 445 wherever possible

3. Windows 10 privacy bug lets users change admin option

Description	
A vulnerability in Windows Diagnostic and Feedback application concerns privilege escalation. The vulnerability is caused by a race condition. The vulnerability was discovered by Arvind Shah, security researcher at FortiGuard Labs. The vulnerability allowed standard user to override the preference setting set by Administrative user in Diagnostic and Feedback application. Security profiles of Defender and SmartScreen are dependent over this preference to deliver various features of security. Standard user, either unknowingly or with malicious intent, could hinder the enhanced protection for all user present on that system.	
Source	https://www.bleepingcomputer.com/news/microsoft/windows-10-privacy-settings-bug-lets-users-change-admin-options/
Infected Technology	Windows 10
CVEs	CVE-2020-1296
Recommendation	Update Windows to the latest patch to address the issue

4. Messenger bug could have helped Malware gain persistence

Description	
Researchers in Reason Cybersecurity disclosed a vulnerability in Facebook's Messenger application for Windows. The vulnerability allowed attacker to leverage the application to execute malicious files already present in the system to provide extended access. The bug was found in Windows Messenger version 460.16 and was addressed quickly via update. The vulnerable application made a call to load Powershell from C:\python27 directory. Researchers created a revere shell disguised as powershell.exe in the defined location to execute the attack.	
Source	https://thehackernews.com/2020/06/facebook-malware-persistence.html
Infected Technology	Messenger for Windows version 460.16
Recommendation	Update to the application version 480.5

5. Black Lives Matter Emails used to deliver TrickBot Malware

Description	
Threat actors are using "Vote for Black Lives Matter" Email to deliver TrickBot Malware. The email contains a word file to vote anonymously for Black Lives Matter. The file when opened is prompted by Microsoft Word, as usual, to enable editing or content. Once allowed, the macros in the document downloads TrickBot in form of malicious library (.DLL file). The TrickBot malware has been gradually extending its function in last few years including collecting user credentials, reconnaissance tool and even backdoors to the affected system.	
Source	https://threatpost.com/black-lives-matter-emails-trickbot-malware/156497/
Infected Technology	Microsoft Word
Recommendation	Do not open attachment from unknown sources Ensure macros are disabled in documents application

6. Two code execution vulnerabilities in Microsoft Excel

Description	
Cisco Talos Researcher recently discovered two code execution vulnerabilities in Microsoft excel that vulnerabilities specially related to the component in Excel that handles the Microsoft Office HTML and XML file types. The vulnerability could be exploited by attacker in a such way that would allow them to execute code on the victim machine after tricking the victim into opening specially crafted excel file.	
Source	https://www.bleepingcomputer.com/news/security/office-365-phishing-baits-remote-workers-with-fake-vpn-configs/
Infected Technology	Microsoft Excel
Recommendation	Update the latest patch released by Microsoft

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**