InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Sound Cloud Suffer Dos and Account Takeover Issues
2. 99 new security flaw was found in Microsoft Windows System
3. Intel to suffer High-Severity Flaw in Security Engine
4. Dell Suffers Support Assist Flaw
5. Mozilla Firefox to suffer high-severity RCE Bugs

17/02/2020

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. Sound Cloud Suffer Dos and Account Takeover Issues

Description	
Sound Cloud is an online music platform for audio-based music creators. Several security bugs have been addressed in its APIs of Sound Cloud. One of the vulnerabilities was authentication issue which could lead to account takeover due to improper input validation. A broken authentication issue with not having set a number of login tries before locking someone out of the account, which can result in unlimited brute-force attacks from attacker trying to guess passwords. Another vulnerability was in /sign-in/password endpoint of api-v2.soundcloud.com, that does not implement proper account lockout based on failed authentication attempts. These vulnerabilities could lead to Denial-of-Service (DoS) or account takeover.	
Source	https://threatpost.com/soundcloud-dos-account-takeover/152838/
Infected Technology	Sound Cloud
Recommendation	Implement rate limiting and resource limiting Implement proper input validation

2. 99 new security flaw was found in Microsoft Windows System

Description	
Microsoft Windows systems suffered 99 security flaws where 12 of the total issues were critical in severity and rest 87 were listed as important. Five of the total issues are still listed as under active attack. The issues include zero-day vulnerability,critical RCE flaw, Remote Desktop client issue,DNS poisoning or Man in the Middle (MITM) attack, LNK shortcuts flaw, and important security feature bypass issues. These vulnerabilities could lead to full control over the victim system with elevated permissions, compromise a legitimate server, host malicious code on victim system,bypass secure boot feature and load untrusted software on the system.	
Source	https://thehackernews.com/2020/02/microsoft-windows-updates.html
Infected Technology	windows 7, 8.1, 10 Windows server 2008,2012,2016,2019 Sql server 2012,2014,2016
Recommendation	Update your device the latest patch released
CVE_ID	CVE-2020-0674 CVE-2020-0662 CVE-2020-0681 CVE-2020-0734 CVE-2020-0729 CVE-2020-0689

3. Intel to Suffer High-Severity flaw in Security Engine

Description	
Intel has faced a high-severity flaw in the firmware of its converged security and management engine (CSME). The flaw was found in the subsystem of CSME that has an improper authentication bug. A privileged user, with local access could exploit the flaw to launch an array of attacks which could allow privilege escalation, denial of service and information disclosure.	
Source	https://threatpost.com/intel-patches-high-severity-flaw-in-security-engine/152794/
Infected Industry	Intel CSME
Recommendation	Update to Intel CSME version to the latest version
CVE_ID	CVE-2019-14598

4. Dell Suffers Support Assist Flaw

Description	
Dell suffers an uncontrolled search path vulnerability in its SupportAssist software. This vulnerability was found on both business PCs version 2.1.3 or older and home PCs version 3.4 or older of dell systems. This vulnerability could allow a locally authenticated user with low privileges to cause loding of arbitrary DLLs by Support Assist binaries which result in privileged execution of arbitrary code to perform overwriting a DLL.	
Source	https://threatpost.com/dell-patches-supportassist-flaw-that-allows-arbitrary-code-execution/152771/
Infected Industry	Dell
Recommendation	Update the
CVE_ID	CVE-2020-5316

5. Mozilla Firefox to suffer high-severity RCE Bug

Description	
Mozilla has faced high-severity memory safety bugs that leave systems open to attack by a remote adversary. These flaws could lead to memory corruption and could be exploited to run arbitrary code. These bugs allow remote attackers to execute code on targeted devices by enticing users to visit a specially-crafted website and exploiting browser memory corruption flaws. This vulnerability stems from a missing bounds check on the shared memory process . command line arguments could be injected during Firefox invocation as a shell handler for certain unsupported file types.	
Source	https://threatpost.com/mozilla-firefox-73-browser-update-fixes-high-severity-rce-bugs/152831/
Infected Technology	Mozilla Firefox 72 Firefox ESR 68.5
Recommendation	Update the latest patch released.
CVE_ID	CVE-2020-6800 CVE-2020-6801

For any queries/recommendations:

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