November 15, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Microsoft patches Excel Zero-day used in attacks
- Ransomware gang exploiting two IE vulnerabilities
- AMD reveals an EPYC 50 flaws – 23 of them classified as high severity
- Zero-day bug in windows
- Phishing campaign using QBot
- MacOS Zero-day used by threat actors to capture keystrokes

CryptoGen Nepal

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.

Microsoft patches Excel Zero-day used in attacks

Description

Microsoft has patched an Excel zero-day vulnerability that threat actors were exploiting in the wild. Excel security hole utilized in last month's Tianfu Cup hacking competition, a remote code execution bug identified as CVE-2021-40442 and exploitable by unauthenticated attackers. This implies that effective exploitation necessitates completely opening maliciously constructed Excel files rather than simply selecting them with a click.

Source	https://www.bleepingcomputer.com/news/microsoft/microsoft-november-2021-patch-tuesday-fixes-6-zero-days-55-flaws/
Infected Technology	Microsoft Excel
Recommendation	Update the latest available patch
CVE_ID	CVE-2021-40442

Ransomware gang exploiting two IE vulnerabilities

Description

Ransomware gang named Magniber has been found exploiting two Internet Explorer vulnerabilities tracked as CVE-2021-26411 and CVE-2021-40444, with severity score of 8.8. The flaws present on the IE is a memory corruption flaw triggered by viewing a specially crafted website and a remote code execution in IE's rendering engine triggered by the opening of a malicious document. The same ransomware gang had also exploited PrintNightmare vulnerability in the pas and are currently actively exploiting Internet Explorer vulnerabilities.

Source	https://www.jioforme.com/magniber-ransomware-group-targets-internet-explorer-vulnerability/917641/
Infected Technology	Internet Explorer
Recommendation	Patch IE to latest release. Apply proper hardening procedures for critical infrastructures with continuous monitoring
CVE_ID	CVE-2021-26411 and CVE-2021-40444

AMD reveals an EPYC 50 flaws – 23 of them classified as high severity

Description	
AMD reveals 50 flaws, 23 of them rated of high severity. The flaws in the AMD Graphics Driver for windows 10 allow privileged escalation, denial of service, the ability for an unprivileged user to drop malicious DLL files onto a system, unauthorized code execution, memory corruption, and information disclosure.	
Source	https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1000
Recommendation	Update the latest available patch.
CVE_ID	CVE-2020-12954, CVE-2020-12961, CVE-2021-26331, CVE-2021-2633, CVE-2021-26334

Zero-day bug in windows

Description	
Microsoft has released an unofficial patch for zero-day for local privilege escalation vulnerability in the Windows User Profile Service that lets attackers gain SYSTEM privileges under certain conditions. The issue impacts all Windows versions including server and host releases.	
Source	https://blog.0patch.com/2021/11/micropatching-incompletely-patched.html
Infected Technology	Microsoft Windows
Recommendation	Apply patches release by Microsoft using opatch agent
CVE_ID	CVE-2021-34484

Phishing campaign using QBot

Description	
Threat Actors have been detected using QBot to launch phishing campaigns via email to lure victims to steal information. QBot was first detected back in 2007 and has been active for more than a decade. The campaign has been seen to provide an Excel file when macros are enabled by the victim which creates a network connection for the deployment of the SquirrelWaffle dropper that causes the download of the QBot in the final stage.	
Source	https://blog.minerva-labs.com/a-new-datoploader-delivers-qakbot-trojan
Infected Technology	Malicious DOC with embedded macros
Recommendation	Phishing awareness campaign and file monitoring on endpoints
CVE-ID	N/A

MacOS Zero-day used by threat actors to capture keystrokes

Description	
Google's Threat Analysis Group has disclosed threat actors are using a zero-day flaw in macOS to spy on people. They stated that a malicious application may be able to execute arbitrary code with kernel privileges. Apple is aware of reports that an exploit for this issue exists in the wild. The exploit used by the threat actors creates an elevation of privilege bug to provide them with a root access on the targeted host.	
Source	https://blog.google/threat-analysis-group/analyzing-watering-hole-campaign-using-macos-exploits/
Infected Technology	• macOS • iOS
Recommendation	Apply patches release by Apple for the selected devices
CVE	CVE-2021-30869

BazarBackdoor abuses Windows 10 app feature to infect victims

Description	
Researchers from Sophos Lab has identified a malware, dubbed BazarBackdoor, that abuses Windows 10 app feature. The malware was spotted when a phishing email was delivered to Sophos Lab's employee. The URL contains PDF preview link that displays a digitally signed software installation prompt, which when allowed, delivers BazarBackdoor malware.	
Source	https://news.sophos.com/en-us/2021/11/11/bazarloader-call-me-back-attack-abuses-windows-10-apps-mechanism/
Infected Technology	Windows 10 Appinstaller, Phishing
Recommendation	Do not click untrusted URLs

Microsoft warns of HTTML smuggling phishing attacks

Description	
Microsoft has seen a surge in malware campaigns using HTML smuggling to distribute banking malware and remote access trojans. The attack uses HTML5 and JavaScript to encode malicious code in a web page. This malicious code is decoded at user end that downloads malicious attachment. These techniques allow attacker to bypass the firewall as the code seems harmless before executed in web browser.	
Source	https://www.microsoft.com/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/
Recommendation	Use endpoint protection to identify malicious files in endpoint

For any queries/recommendations:
Contact us: **whois@cryptogennepal.com**

OUR SERVICES

Our services as information security company includes:

- INFORMATION SECURITY AUDIT
- VULNERABILITY ASSESSMENT
- PENETRATION TESTING
- MANAGED/CO.MANAGED SOC
- INCIDENT RESPONSE
- THREAT ANALYSIS
- SERVER HARDENING
- CYBER SECURITY CONSULTANT
- INFORMATION SECURITY TRAINING

CryptoGen Nepal

https://www.facebook.com/CryptoGenNepal/
https://twitter.com/CryptoGenNepal
https://www.instagram.com/CryptoGenNepal/