August 15, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Palo Alto Networks Firewalls Targeted for Reflected, Amplified DDoS Attacks.
- Xiaomi phones with MediaTek chips vulnerable to forged payments
- Mass Exploitation of Zimbra RCE vulnerability
- Researchers Uncover UEFI Secure Boot Bypass in 3 Microsoft Signed Boot Loaders

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.

Palo Alto Networks Firewalls Targeted for Reflected, Amplified DDoS Attacks.

Description	
Palo Alto Networks is working on fixes for a reflected amplification denial-of-service (DoS) vulnerability that impacts PAN-OS, the platform powering its next-gen firewalls. The company has learned that a threat actor has attempted to abuse firewalls from multiple vendors for distributed denial-of-service (DDoS) attacks. No additional information appears to be available on these attacks and the other impacted firms. "Palo Alto Networks recently learned that an attempted reflected denial-of-service (RDoS) attack was identified by a service provider. This attempted attack took advantage of susceptible firewalls from multiple vendors, including Palo Alto Networks," the company says.	
Source	https://www.securityweek.com/palo-alto-networks-firewalls-targeted-reflected-amplified-ddos-attack
Infected Technology	Palo Alto Network Firewall (PAN-OS 10.1)
Recommendation	Enable packet-based attack protection or flood protection.
CVE_ID	CVE-2022-0028 (CVSS score of 8.6)

Xiaomi phones with MediaTek chips vulnerable to forged payments

Description	
Security experts have discovered vulnerabilities in Xiaomi devices` payment systems, which depend on MediaTek processors to provide the trusted execution environment (TEE) necessary for signing transactions. Such an assault would have the potential to sign transactions from the user's mobile wallet to the threat actor's account or disable the payment service. Another flaw in the Tencent Soter trusted app that enables an attacker to harvest private keys and sign phony payment packages while operating in the context of an ordinary user was exploited by the researchers.	
Source	https://www.bleepingcomputer.com/news/security/xiaomi-phones-with-mediatek-chips-vulnerable-to-forged-payments/
Infected Technology	Xiaomi phones with MediaTek chips
Recommendation	Apply June Android 2022 security updates
CVE_ID	CVE-2020-14125

Mass Exploitation of Zimbra RCE vulnerability

Description	
The United States Cybersecurity and Infrastructure Security Agency (CISA) added two flaws to its Known Exploited Vulnerabilities Catalog on Thursday, citing active exploitation. The two high-severity issues are related to Zimbra Collaboration flaws, which could be linked together to allow unauthenticated remote code execution on affected email servers. CVE-2022-27925(CVSS value: 7.2)- Remote code execution (RCE) from an authenticated user via mboximport and CVE-2022-37042- MailboxImportServlet authentication bypass. The disclosure comes a week after CISA added another Zimbra-related bug, CVE-2022-27924, to the catalog, which, if exploited, could allow attackers to steal cleartext credentials from users of the targeted instances.	
Source	https://thehackernews.com/2022/08/researchers-warn-of-ongoing-mass.html
Infected Technology	Versions below 8.8.15 Patch 33 and 9.0.0 Patch 26
Recommendation	Update to latest version (8.8.15 Patch 33 and 9.0.0 Patch 26)
CVE_ID	CVE-2022-27925, CVE-2022-37042

Researchers Uncover UEFI Secure Boot Bypass in 3 Microsoft Signed Boot Loaders

Description	
Security feature bypass vulnerability has been uncovered in three signed third-party Unified Extensible Firmware Interface (UEFI) boot loaders that allow bypass of the UEFI Secure Boot feature. The vulnerability can be exploited by mounting the EFI System Partition and replacing the existing bootloader with the vulnerable one or modifying a UEFI variable to load the vulnerable loader instead of the existing one. This vulnerability can enable a bad actor to gain entrenched access and establish persistence on a host in a manner that can survive operating system reinstalls and hard drive replacements as well as completely bypass detection by security software.	
Source	https://thehackernews.com/2022/08/researchers-uncover-uefi-secure-boot.html
Infected Technology	Microsoft Teams
Recommendation	• Update to the latest version
CVE_ID	CVE-2022-34301, CVE-2022-34302, CVE-20220-34303

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/