September 19, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- WAPPLES web application firewall faulted for multiple flaws
- WordPress Sites Hacked via Zero-Day Vulnerability in WP-Gateway Plugin.
- High-Severity Vulnerabilities in HP Enterprise Devices Remain Unpatched.
- Uber hack linked to hardcoded secrets spotted in powershell script
- SAP Patches High-Severity Flaws in Business One, BusinessObjects, GRC

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.

WAPPLES web application firewall faulted for multiple flaws

Description	
Researcher warns for multiple vulnerability in the WAPPLES web application firewall (WAF) created a means to commandeer vulnerable devices and run arbitrary command. The vulnerability allows a remote attacker to execute arbitrary code or obtain confidential information using predefined credentials, among other exploits. The researcher also discovered that it was possible to escalate user privileges to root in versions 5.0 and 6.0 of the technology. WAPPLES uses a vulnerable CouchDB version in default configuration that leads to remote OS command execution and to exploit this vulnerability the attacker must have access to the management interface. The attack could also gain unprivileged access to a system as a 'couchdb' user, then escalate privileges using the other vulnerabilities.	
Source	https://portswigger.net/daily-swig/wapples-web-application-firewall-faulted-for-multiple-flaws
Infected Technology	WAPPLES web application firewall
Recommendation	Update to latest version
CVE_ID	CVE-2022-24706, CVE-2022-31322, CVE-2022-35413, CVE-2022-31324, and CVE-2022-35582

WordPress Sites Hacked via Zero-Day Vulnerability in WP-Gateway Plugin.

Description	
Many WordPress sites are at risk of full compromise as attackers are actively exploiting a zero-day vulnerability in the WP-Gateway plugin. A premium plugin for the WP-Gateway cloud service, the WP-Gateway plugin provides users with WordPress installation, backup, and cloning capabilities. Tracked as CVE-2022-3180 (CVSS score of 9.8), the recently identified vulnerability allows an unauthenticated attacker to add an administrator account to websites running WPGateway. if an administrator account with the username 'rangex' appears in the dashboard, it means that the WordPress site has been compromised. Site owners may also check the site's access logs for specific requests indicating that they have been targeted.	
Source	https://www.securityweek.com/wordpress-sites-hacked-zero-day-vulnerability-wpgateway-plugin
Infected Technology	WordPress sites using WP-Gateway.
Recommendation	Continuously monitor for any indication of compromise.
CVE_ID	CVE-2022-3180

High-Severity Vulnerabilities in HP Enterprise Devices Remain Unpatched.

Description	
During Black Hat USA conference in mid-August 20222, details for various high severity vulnerabilities in HP's business-oriented high-end notebooks were disclosed. These weaknesses are a case of memory corruption in the System Management Module (SMM) of the firmware. According to Binarly, the vulnerabilities "can't be detected by firmware integrity monitoring systems due to limitations of the Trusted Platform Module (TPM) measurement". The firmware vulnerability can help an adversary achieve long term persistence and code execution in the highest privilege. These vulnerabilities continue to remain unpatched even months after public disclosure.	
Source	https://support.hp.com/us-en/document/ish_5817864-5817896-16/hpsbhf03776
Infected Technology	HP EliteBook series, HP ProBook Series, various HP Thunderbolt Dock models, HP ZBook series, HP ZHAN series, various models of HP Elite Slice, HP EliteDesk series, HP EliteOne series, HP ProDesk series, various models of HP Engage Flex Retail system, Various models of HP Client PCs and Workstations,
Recommendation	Contact HP customer support and update to the latest firmware after it is available.
CVE_ID	CVE-2022-23924, CVE-2022-23925, CVE-2022-23930, CVE-2022-23931, CVE-2022-23934, CVE-2022-23926, CVE-2022-23927, CVE-2022-23928, CVE-2022-23929

Uber hack linked to hardcoded secrets spotted in powershell script

Description
Uber is looking into accusations that an intruder has compromised company systems. By uploading screenshots and commenting on their exploits in discussions with the media and security experts, the attacker demonstrated that they had successfully hacked many of the ride-sharing app firm's internal networks. The miscreant stated that they used social engineering to acquire access to an employee's VPN credentials. This unauthorized access enabled them to break into Uber's network and scan its intranet. Uber is said to use multi-factor authentication (MFA). According to third-party experts, an attacker may have been able to evade these protections by creating a bogus domain and relaying authentication tokens submitted to the legitimate domain via a man-in-the-middle (MitM) attack.

Source	https://portswigger.net/daily-swig/uber-hack-linked-to-hardcoded-secrets-spotted-in-powershell-script
Infected Technology	Uber Internal Network
Recommendation	Stay up to date with Security news related to Uber

SAP Patches High-Severity Flaws in Business One, BusinessObjects, GRC

Description
German software maker SAP this week announced the release of eight new and five updated security notes as part of its September 2022 Security Patch Day. The most important of the newly released security notes deals with a high-severity vulnerability in Business One that could lead to escalation of privileges. SAP also addressed a high-severity vulnerability in BusinessObjects (CVE-2022-39014, CVSS score of 7.7), which could provide an attacker with access to unencrypted sensitive information. All the five remaining new security notes released on SAP's September 2022 Security Patch Day are rated 'medium severity'. They impact BusinessObjects, NetWeaver Enterprise Portal, NetWeaver AS ABAP, and NetWeaver Application Server ABAP.

Source	https://www.securityweek.com/sap-patches-high-severity-flaws-business-one-businessobjects-grc
Infected Technology	BusinessObjects NetWeaver Enterprise Portal NetWeaver AS ABAP NetWeaver Application Server ABAP
Recommendation	Update to the latest version and patch the vulnerability.
CVE_ID	CVE-2022-35292 CVE-2022-39801 CVE-2022-39014

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