August 29, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- CISA Warns of Active Exploitation of Palo Alto Networks' PAN-OS Vulnerability
- Over 80,000 exploitable Hikvision cameras exposed online
- Gitlab remote command execution vulnerability.
- Mozilla Patches High-Severity Vulnerabilities in Firefox, Thunderbird.
- Remote code execution vulnerability discovered in Atlassian Bitbucket Server and Data Center

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.

CISA Warns of Active Exploitation of Palo Alto Networks' PAN-OS Vulnerability	
Description	
Unauthenticated, remote attackers may be able to conduct reflected and amplified TCP denial-of-service (DoS) attacks due to a URL filtering policy misconfiguration, which is a high-severity vulnerability. The availability, confidentiality, or integrity of our goods would not be affected if this problem were to be exploited. Attacks that cause a denial-of-service (DoS) may make it difficult to identify the perpetrator and point the finger at the firewall as the attack's origin.	
Source	https://thehackernews.com/2022/08/cisa-warns-of-active-exploitation-of.html
Infected Technology	Palo Alto Networks PAN-OS
Recommendation	• update to the latest version
CVE_ID	CVE-2022-0028

Over 80,000 exploitable Hikvision cameras exposed online

Description	
80,000 Hikvision cameras were discovered vulnerable to a critical command injection flaw which can be easily exploited via specially crafted messages sent to the vulnerable web server. It is found that tens of thousands of systems used by 2,300 organizations across 100 countries have still not applied the security update. The exploitation of flaws does not follow a specific pattern and it is believed that by using vulnerable Hikvision camera products cybercriminals from countries launch geopolitically motivated cyber warfare. Along with command injection vulnerability, there is also the issue of weak passwords that users set for convenience or that come with device by default and aren't reset during the first step.	
Source	https://www.bleepingcomputer.com/news/security/over-80-000-exploitable-hikvision-cameras-exposed-online/
Infected Technology	Hikvision cameras
Recommendation	• Install latest available firmware update. • Use strong Password and isolate IoT network
CVE_ID	CVE-2021-36260

Gitlab remote command execution vulnerability.

Description	
With a CVSS score of 9.9, GitLab formally released a security alert to address a significant vulnerability (CVE-2022-2884) in the Community Edition (CE) and Enterprise Edition (EE). An open-source project for a warehouse management system is called GitLab. It makes use of Git as a code management technology to provide web-based access to both public and private projects. An authenticated person could exploit this issue to execute code remotely by using the Import from GitHub API endpoint.	
Source	https://securityonline.info/cve-2022-2884-gitlab-remote-code-execution-vulnerability/
Infected Technology	• Gitlab CE/EE from 11.3.4 to before 15.1.5 • Gitlab CE/EE 15.2 prior to 15.2.3 • Gitlab CE/EE 15.3 prior to 15.3.1
Recommendation	Update to latest patched versions: • Gitlab CE/EE 15.1.5 • Gitlab CE/EE 15.2.3 • Gitlab CE/EE 15.3.1
CVE_ID	CVE-2022-2884

Mozilla Patches High-Severity Vulnerabilities in Firefox, Thunderbird.	
Description	
Firefox 104 — as well as Firefox ESR 91.13 and 102.2 — patches a high-severity address bar spoofing issue related to XSLT error handling. The flaw, tracked as CVE-2022-38472, could be exploited for phishing. The latest Firefox release also resolves CVE-2022-38473, an issue related to cross-origin XSLT documents that could pose security and privacy risks. In addition, two CVE identifiers, CVE-2022-38477 and CVE-2022-38478, have been assigned to multiple memory safety bugs that could lead to arbitrary code execution.	
Source	https://www.securityweek.com/mozilla-patches-high-severity-vulnerabilities-firefox-thunderbird-0
Infected Technology	Mozilla Firefox ESR, Thunderbird.
Recommendation	Update to latest version and patch the vulnerability.
CVE_ID	CVE-2022-38472 CVE-2022-38473

Remote code execution vulnerability discovered in Atlassian Bitbucket Server and Data Center

Description	
Atlassian recently released patches for a critical vulnerability in their Bitbucket Server and Data Center. This vulnerability could allow a remote attacker to achieve remote code execution (RCE). According to Atlassian "An attacker with access to a public Bitbucket repository or with read permissions to a private one can execute arbitrary code by sending a malicious HTTP request". In scenarios where patches cannot be applied immediately, Atlassian suggests turning off public repositories using "feature.public.access=false" to prevent unauthenticated users from exploiting the flaw.	
Source	https://thehackernews.com/2022/08/critical-vulnerability-discovered-in.html
Infected Technology	all versions of Bitbucket Server and Datacenter released after 6.10.17, inclusive of 7.0.0 and newer: • Bitbucket Server and Datacenter 7.6 • Bitbucket Server and Datacenter 7.17 • Bitbucket Server and Datacenter 7.21 • Bitbucket Server and Datacenter 8.0 • Bitbucket Server and Datacenter 8.1 • Bitbucket Server and Datacenter 8.2, and • Bitbucket Server and Datacenter 8.3
Recommendation	Update to latest version and patch the vulnerability, or apply the workaround by turning off public repositories
CVE_ID	CVE-2022-36804

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