August 8, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Authentication bypass bug in Nextauth.js could allow email account takeover
- Jenkins security: Unpatched XSS, CSRF bugs included in latest plugin advisory
- ZIMBRA email vulnerabilities added to CISA catalog
- Critical Vulnerabilities Allow Hacking of Cisco Small Business Routers.

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.

Authentication bypass bug in Nextauth.js could allow email account takeover

Description

A critical authentication bypass flaw in an NPM package was discovered in NPM packet which could allow a malicious actor to take over a victim’s email account. The vulnerability present in Nextauth.js, is an open source authentication package for next.js applications. Users on NPM package-auth who are using the Email Provider either in versions before 4.10.3 or 3.29.10 are affected by the bug. The attacker could login as a newly created user if an attacker could forge a request that sent a comma-separated list of emails, to the sign-in endpoint, Nextauth.js would send emails to both attacker and to the victim’s email addresses.

Source	https://portswigger.net/daily-swig/authentication-bypass-bug-in-nextauth-js-could-allow-email-account-takeover
Infected Technology	Nextauth.js
Recommendation	Update to latest version

XSS vulnerabilities in Google Cloud, Google Play could lead to account hijacks

Description

A pair of flaws in Google Cloud, DevSite, and Google Play might have enabled attackers to launch cross-site scripting (XSS) attacks, potentially leading to account hijacking. The first flaw is a mirrored XSS flaw in Google DevSite. An attacker-controlled link might invoke JavaScript on the origins http://cloud.google.com and http://developers.google.com, allowing a malicious actor to view and alter its contents while circumventing the same-origin restriction. The second vulnerability is a DOM-based XSS on Google Play. DOM-based XSS vulnerabilities usually arise when JavaScript takes data from an attacker-controllable source, such as the URL, and passes it to a sink that supports dynamic code execution, such as eval() or innerHTML. This enables attackers to execute malicious JavaScript, which typically allows them to hijack other users' accounts.

Source	https://portswigger.net/daily-swig/xss-vulnerabilities-in-google-cloud-google-play-could-lead-to-account-hijacks
Infected Technology	Version below latest security patches
Recommendation	Already fixed by Google, stay up-to-date with security news.

Jenkins security: Unpatched XSS, CSRF bugs included in latest plugin advisory

Description

Jenkins, an open-source DevOps platform, has issued a security advisory to users about unpatched vulnerabilities that affect more than a dozen plugins. Jenkins is a well-known open-source automation server that offers a huge selection of plugins to help with creating, delivering, and automating projects. There are a total of 27 plugin vulnerabilities listed in the organization's most recent security alert, five of which were rated as having a "high" impact, and the rest of which are still unpatched. A cross-site request forgery (CSRF) vulnerability in the Coverity plugin tops the list of high impact flaws, all of which were unfixed as of the time of writing. In the meanwhile, a vulnerability in the CLIF Performance Testing Plugin that permits arbitrary file writing enables attackers with 'Overall/Read' access to create or alter any file on the Jenkins controller file system with malicious code. Along with a reflected XSS bug in the Lucene-Search plugin, further cross-site scripting (XSS) vulnerabilities were found in the Dynamic Extended Choice Parameter and Maven Metadata plugins.

Source	https://portswigger.net/daily-swig/jenkins-security-unpatched-xss-csrf-bugs-included-in-latest-plugin-advisory
Infected Technology	CLIF Performance Testing Plugin, Dynamic Extended Choice Parameter plugin, Lucene-Search plugin
Recommendation	Uninstall the plugin
CVE_ID	CVE-2022-36894, CVE-2022-36902, CVE-2022-36905, CVE-2022-36922

ZIMBRA email vulnerabilities added to CISA catalog

Description

The recently disclosed high severity (CVSS score: 7.5) vulnerability in ZIMBRA email suite as added by Cybersecurity and Infrastructure agency (CISA) to its known exploited vulnerabilities catalog due to evidences of active exploitation. The vulnerability, tracked as CVE-2022-27924, could lead to theft of sensitive information via command injection. According to CISA " Zimbra Collaboration (ZCS) allows an attacker to inject memcached commands into a target instance which causes an overite of arbitrary cached entries." This issue was disclosed in june by cybersecurity firm, SonarSource. Zimbra released patches in May 2022.

Source	https://thehackernews.com/2022/08/cisa-adds-zimbra-email-vulnerability-to.html
Infected Technology	Zimbra Web client
Recommendation	• Update to versions 8.8.15 P31.1 and 9.0.0 P24.1
CVE_ID	CVE-2022-27924

Critical Vulnerabilities Allow Hacking of Cisco Small Business Routers.

Description

Updates released by Cisco for some of its small business routers patch serious vulnerabilities that could allow threat actors to take control of affected devices. Three vulnerabilities have been identified by external researchers in Cisco's RV160, RV260, RV340, and RV345 series VPN routers. An unauthenticated attacker could exploit the flaws remotely for arbitrary code execution and denial-of-service (DoS) attacks. Two of the vulnerabilities have been assigned a 'critical' severity rating. One of them, CVE-2022-20842, affects the routers' web-based management interface and is caused by insufficient user input validation. The second critical security hole, CVE-2022-20827, affects the routers' web filter database update feature..

Source	https://www.securityweek.com/critical-vulnerabilities-allow-hacking-cisco-small-business-routers
Infected Technology	Cisco RV160, RV260, RV340, and RV345 series VPN routers
Recommendation	Update to the latest security patch released by cisco.
CVE_ID	CVE-2022-20842 CVE-2022-20827 CVE-2022-20841

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