March 1, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- VMware fixes critical RCE bug in vSphere and ESXi
- Cisco fixes Cisco ACI MSO auth bypass vulnerability
- Mozilla Patches Bugs in Firefox, Now Blocks Cross-Site Cookie Tracking
- Popular Node.js package vulnerable to command injection attacks
- Malicious Mozilla Firefox Extension Allows Gmail Takeover

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.

1. VMware fixes critical RCE bug in vSphere and ESXi

Description	
VMware has rectified the critical remote code execution (RCE) vulnerability in its vCenter Server virtual infrastructure management platform. The vulnerability was initially rated as the base score of 9.8 out of 10 allowed potential attackers to take control of the affected system. The successful exploitation could be achieved remotely by unauthenticated attackers in low complexity attacks which do not require user interaction. The remote code execution vulnerability resides in the vCenter Server plugin. The malicious users with network access on port 443 may exploit the vulnerability for executing commands with unrestrictive privileges on the operating system hosting the vCenter Server. Proof-of-Concept code has been released by various researchers allowing various malicious users to exploit the vulnerability. VMware has rectified a heap-overflow bug in ESXi's service location protocol (SLP). The OpenSLP framework allows the network applications to discover the existence, configuration of networked services and location in the enterprise network infrastructure. The bug in SLP allowed potential attackers within the same network to send malicious SLP request to the ESXi devices. The request could potentially take control of the affected ESXi endpoint. The SLP could be leveraged to trigger the use-after-free OpenSLP service that leads to remote code execution (RCE). A Server-Side Request Forgery (SSRF) vulnerability was identified in vSphere Client (HTML5). The vulnerability was a result of the improper validation of URLs present in the vCenter Server plugin. A malicious user with the network access of port 443 of the affected endpoint could exploit the issue. The exploit was possible by sending a POST request to the vCenter Server plugin. The result of this exploitation could lead to information disclosure of the vulnerable endpoint.	
Source	https://kb.vmware.com/s/article/82374
Infected Technology	VMware vCenter Server, ESXi and vCenter Server 7.0
CVE ID	CVE-2021-21972, CVE-2021-21973, CVE-2021-21974
Recommendation	• Consider upgrading the affected installation to vCenter Server 6.5 U3n, 6.7 U3l or 7.0 U1c. • If not able to upgrade, apply the workaround provided in the advisory. • Consider installing the latest VMware ESXi updates. • Consider installing the latest patch of vCenter Server (7.0 U1c)

2. Cisco fixes Cisco ACI MSO auth bypass vulnerability

Description

Cisco has fixed maximum severity authentication bypass vulnerability in the API endpoint of Cisco ACI Multi-Site Orchestrator (MSO) on the Application Services Engine. The vulnerability in the API endpoint allowed unauthenticated remote attackers to bypass the authentication procedure in the affected devices. The improper token validation bug could be exploited with a crafted request by the unauthenticated attacker. The successful exploitation of this vulnerability allowed an attacker to get an unauthenticated token with admin-level privileges. The token was then used for authenticating to the API on the affected MSO and for managing Cisco Application Policy Infrastructure Controller (APIC) devices.

Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mso-authbyp-bb5GmBQv
Infected Technology	Cisco ACI MSO 3.0
CVE ID	CVE-2021-1388
Recommendation	Consider upgrading the installation to Cisco ACI MSO 3.0 (3m)

3. Mozilla Patches Bugs in Firefox, Now Blocks Cross-Site Cookie Tracking

Description

The Mozilla Foundation has released its latest version of the Firefox browser, which comes with new privacy protections to squash cross-site cookie tracking, as well as a few security vulnerabilities fixes. Firefox 86, released on Tuesday, includes what it touts as a privacy-bolstering feature called Total Cookie Protection. This new feature isolates each cookie assigned by each website – preventing websites from tracking internet users in an invasive, cross-site manner. Total Cookie Protection confines cookies to the site where they were created, which prevents tracking companies from using these cookies to track users browsing from site to site. However, few momentary exceptions are applied that allow for strong privacy protection without affecting users' browsing experience.

Source	https://blog.mozilla.org/security/2021/02/23/total-cookie-protection/
Infected Technology	Mozilla Firefox version < 86
CVE ID	CVE-2021-23969, CVE-2021-23970, CVE-2021-23968
Recommendation	Confider upgrading Mozilla Firefox to its latest version.

4. Popular Node.js package vulnerable to command injection attacks

Description

The maintainers of systeminformation, a popular Node.js package, have patched a bug that left applications vulnerable to command injection attacks. Systeminformation provides dozens of functions for retrieving detailed hardware, system, and operating system information from servers hosting Node.js applications. The library has more than 850,000 weekly downloads on NPM, the main online repository for Node.js packages. Four functions in systeminformation were found to be vulnerable to command injection. According to Hildebrandt, the maintainer of the software, the vulnerability was caused due to a special case of improper parameter checking and array sanitation. The vulnerability now has been fixed in the latest version of systeminformation.

Source	https://github.com/advisories/GHSA-2m8v-572m-ff2v
Infected Technology	Systeminformation (npm) version < 5.3.1
CVE ID	CVE-2021-21315
Recommendation	Consider updating Node.js to its latest version.

5. Malicious Mozilla Firefox Extension Allows Gmail Takeover

Description

A newly uncovered cyberattack is taking control of victims' Gmail accounts, by using a customized, malicious Mozilla Firefox browser extension called FriarFox. After installation, FriarFox gives cybercriminals various types of access to users' Gmail accounts and Firefox browser data. According to the researchers, the users must access the URL from a Firefox browser to receive the browser extension. Additionally, it appeared that the user must be actively logged in to a Gmail account within that browser to successfully install the malicious XPI [FriarFox] file. The users are prompted to add the browser extension, which claims to be 'Flash update components. Once installed the attack becomes successful and victims' Gmail account gets compromised.

Source	https://www.proofpoint.com/us/blog/threat-insight/ta413-leverages-new-friarfox-browser-extension-target-gmail-accounts-global
Infected Technology	Firefox Web Browser
Recommendation	Consider not using the FriarFox browser extension.

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**