z

July 19, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Threat actors actively attacking SolarWinds zero-day vulnerability
- Linux varient of HelloKitty ransomware
- CDN flaw in cloudflare considered critical
- Critical juniper Bug Allows DoS, RCE Against Carrier Networks
- Google Chrome fixes 0-day exploited in the wild
- D-Link releases hotfix for hard-coded router password
- Windows Print Spooler vulnerable to Privilege escalation
- Adobe updates fix 28 vulnerabilities in 6 programs

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.

Threat actors actively attacking SolarWinds zero-day vulnerability

Description

Recently, the news broke out regarding mass supply chain attack where threat actors were observed utilizing vulnerability on SolarWinds platform. An RCE vulnerability in Serv-U managed file transfer service provided by SolarWinds is being exploited. The current flaw on Serv-U affects from the version 15.2.3 and prior. If any attacker successfully exploits this vulnerability, then the attacker can run arbitrary code on the infected system.

Source	https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
Infected Technology	SolarWinds
Recommendation	Keep a look out for the following IPs 98[.]176[.]196[.]89 and 68[.]235[.]178[.]32 or 208[.]113[.]35[.]58 via TCP 443. and keep reviewing cybersecurity posture at regular intervals.
CVE-ID	CVE-2021-35211

Linux varient of HelloKitty ransomware

Description

A Linux variant of the HelloKitty ransomware was used to launch attacks against VMware ESXI systems. @malwarehunterteam discovered numerous Linux ELF-64 versions of the HelloKitty ransomware targeting VMware ESXi servers and virtual machines running on them. There seems to be other variant of Linux encryptors targeting ESXi VMs such as Babuk, RansomExx, GoGoogle and others.

Source	https://securityaffairs.co/wordpress/120158/cyber-crime/hellokitty-ransomware-linux-variant.html
Infected Technology	Linux Systems, VMware ESXi
Recommendation	Frequently patch updates to your ESXi servers. Monitor changes occuring on ESXi.
CVE-ID	N/A

CDN flaw in cloudflare considered critical

Description	
Cloudflare recently patched a critical vulnerability in its free and open-source CDNJS which is set to impact 12.7% of all websites on the internet. This service hosts millions of websites with over 4000 JavaScripts and the addressed vulnerability can be leveraged by threat actors to trigger a Path Traversal vulnerability and eventually RCE (Remote Code Execution).	
Source	https://www.bleepingcomputer.com/news/security/critical-cloudflare-cdn-flaw-allowed-compromise-of-12-percent-of-all-sites/
Infected Technology	CloudFlare
Recommendation	N/A
CVE-ID	N/A

Critical juniper Bug Allows DoS, RCE Against Carrier Networks

Description	
A critical remote code-execution vulnerability in Juniper Networks' Steel-Belted Radius (SBR) Carrier Edition lays open wireless carrier and fixed operator networks to tampering. By centralizing user authentication, giving the proper level of access, and verifying compliance with security standards, telecom carriers utilize the SBR Carrier server to manage policies for how subscribers use their networks. It enables carriers to distinguish service tiers, diversify revenue models, and manage network resources. According to Juniper's advisory, it's a stack-based buffer-overflow vulnerability that an attacker can exploit by sending specially designed packets to the platform, causing the RADIUS daemon to crash which can cause RCE as well as denial-of-service (DoS), which prevents phone subscribers from connecting to the internet.	
Source	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11180&cat=SIRT_1&actp=LIST
Infected Technology	Juniper Networks SBR Carrier: • 8.4.1 versions prior to 8.4.1R19 • 8.5.0 versions prior to 8.5.0R10 • 8.6.0 versions prior to 8.6.0R4.
Recommendation	Update the latest available patch.
CVE-ID	CVE-2020-0276

Google Chrome fixes 0-day exploited in the wild

Description

Google has released a new update for its browser for Windows, Linux and Mac that fixes 0-day being exploited in the wild. The patch fixes eight issue out of which six are of high severity. Google has not released the details of the bug until majority of the user has updated to latest patched version.

Source	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html
Infected Technology	CVE-2021-30559, CVE-2021-30541, CVE-2021-30560, CVE-2021-30561, CVE-2021-30562, CVE-2021-30563, CVE-2021-30564
Recommendation	Update to 91.0.4472.164
CVE-ID	N/A

D-Link releases hotfix for hard-coded router password

Description

D-Link has released a hotfix for its firmware to address multiple vulnerability in DIR-3040 wireless router. The vulnerability allows threat actor to execute arbitrary code in unpatched router, access sensitive information or cause denial of service. Hard coded password vulnerability in Zebra IP Routing Manager allows users to bypass authentication configured by software administrator.

Source	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10228
Infected Technology	D-Link 3040
Recommendation	Apply the hotfix released by D-Link
CVE-ID	CVE-2021-21816, CVE-2021-21817, CVE-2021-21818, CVE-2021-21819, CVE-2021-21820

Windows Print Spooler vulnerable to Privilege escalation

Description	
Microsoft has announced yet another vulnerability in its Print spooler service which allows escalation of privilege to SYSTEM level. The vulnerability is considered independent from PrintNightmare, previous vulnerability in the service. The issue has not been fixed and technical details regarding the vulnerability has not been released. The discussion of the vulnerability is teased to be announced in DEFCON while no statement has been provided by Microsoft on the issue.	
Source	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481
Infected Technology	Microsoft Windows
Recommendation	• Disable Print Spooler service • Apply update after the patch has been released
CVE-ID	CVE-2020-34481

Adobe updates fix 28 vulnerabilities in 6 programs

Description	
Adobe, a multinational computer software firm based in the United States, has released a large Patch Tuesday security update that addresses vulnerabilities in Adobe products such as Dimension, Illustrator, Framework, Acrobat, Reader, and Bridge. All of the patches address a critical vulnerability. If these weaknesses are successfully exploited, hackers may be able to execute arbitrary code on vulnerable devices, allowing them to carry out orders.	
Source	https://heimdalsecurity.com/blog/security-alert-surprise-adobe-patch-eliminates-critical-flaw-in-acrobat-and-reader/
Infected Technology	• Adobe Dimension version 4.3 and earlier • Adobe Illustrator version 25.2.3 and earlier • Adobe Framework version 2020 Release Update 1 and earlier and 2019 Update 8 and earlier • Adobe acrobat and reader • Adobe Bridge 11.0.2 and earlier versions
Recommendation	Update the latest patch available
CVE-ID	N/A

Windows Hello Security Feature Bypass Vulnerability

Description

Windows Hello is a feature in Windows 10 that allows users to authenticate a device without entering a password by using a PIN number or biometric identification (either a fingerprint or face recognition). The researchers revealed that attackers may use a single legitimate IR (infrared) frame of the target to totally defeat Windows Hello's face recognition system by creating bespoke USB devices that Windows Hello would operate with.

Source	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34466
Infected Technology	Windows
Recommendation	Update the latest available patch
CVE-ID	CVE-2021-34466

WooCommerce plugin vulnerability impacts 5 million sites to data theft

Description

WooCommerce, the popular e-commerce plugin for WordPress has released a new update that fixes critical vulnerability. The vulnerability is an SQL injection vulnerability that allows attacker to obtain store-related information, administrative details and data of customers and order. The vulnerability is now being exploited in the wild. Developers are urged to update the plugin to the latest patch version.

Source	https://woocommerce.com/posts/critical-vulnerability-detected-july-2021/
Infected Technology	WooCommerce version 3.3 through 5.5; WooCommerce Blocks 2.5 through 5.5
Recommendation	Update the latest available patch.
CVE-ID	N/A

Several Vulnerabilities Patched in 'MDT AutoSave’

Description	
MDT, an automation change management solution used by some of the world's largest manufacturers was discovered to be affected by seven vulnerabilities. The vulnerabilities in their flagship product included two critical and five high severity variations. According to the Vulnerability Research Team at Claroty, an attacker needs network access to the MDT AutoSave server in order to exploit the vulnerabilities. MDT Software has patched these several critical and high-severity vulnerabilities in MDT AutoSave.	
Source	https://www.securityweek.com/several-vulnerabilities-patched-mdt-autosave-industrial-automation-product?&web_view=true
Infected Technology	MDT AutoSave
Recommendation	Update the latest available patch.
CVE-ID	CVE-2021-32953, CVE-2021-32933,

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/